View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by NORA - Norwegian Open Research Archives

AIR PASSENGER DATA PROTECTION

Data Transfer from the European Union to the United States

Candidate number: 12

Supervisor: Jon Bing

Deadline for submission: 28 September 2009

Number of words: 17,936

15 September 2009

UNIVERSITY OF OSLO

Faculty of Law

Content

1 Introduction

Within the recent history, the world has experienced dramatic events which had a substantial effect on the balance (or, alternatively, the "struggle") between data protection[1] and security measures. This "struggle" can be clearly seen in the issues of data transfer from the European Union (EU) to the United States of America (US).

The right to privacy and data protection belongs to the fundamental rights and freedoms of the individuals. Historically, the EU had a tendency to enact strict and broad data protection laws. The most comprehensive and substantial of the adopted legal instruments is the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data (Directive), which establishes data protection rules and principles according to high level standards.

There was a similar tendency in the US, especially after the development of the Internet and the demands for protection of personal information, but the tragic events of 11 September 2001 dramatically changed American life. The terrorist attacks forced the US to "barter" civil liberties for increased national security, introducing enhanced anti-terrorism legislation. New surveillance and control measures, including the collection of personal information, were enforced under the motto of combating terrorism.

[1] The term "data protection" is most commonly used in European jurisdictions; in the US, the term "privacy protection" tends to be used instead. See: Bygrave, Lee A. *Data Protection Law: Approaching Its Rationale, Logic and Limits,* Kluwer Law International (2002).

Therefore, a conflict arose between the EU and the US. The Directive made it difficult for the US to collect data from Europe without violating the EU law. The EU representatives recognized and valued the underlying goals of the US's anti-terrorism legislation, but nonetheless insisted on compatibility with European laws. The "struggle" between the US demands for access to information and the EU data protection compliance obligations commenced. The principal issue was as follows: how much of European air passenger personal data should be shared with the US authorities and under which conditions should this take place?

The first part of chapter 2 of this work examines the actual problem, its background, as well as the key terms and legal instruments. The second part discusses and analyses, in chronological order, the development of "solution" of the problem proposed by the parties: the EU-US agreement of 2004 (annulled by the European Court of Justice), the interim agreement of 2006, and, finally, the current agreement of 2007. In the third part, different issues concerning further development of the situation will be discussed, including the US additional requirements and demands beyond the scope of the EU-US agreement, as well as further steps and proposals. The forth part analyses the proposed EU system, which is currently under discussion within the EU (the plan is similar to the EU-US scheme), and other plans aimed in stronger security measures enforcement.

Chapter 3 is a summary of the issues discussed in the work. It concludes by pointing out the unlawfulness of former and current data transfers and sets forth the author's perspective on how the overarching problem can be resolved while still respecting the United States' desire of security from terrorists and the EU desire for protection of its citizen's privacy.

2 Text Material

2.1 The Problem

2.1.1 Background

It is believed that the story of hijacking as a threat for civil aviation and the fight against it started in 1968, when the world faced the problem of politically motivated aircraft terrorists. As the result, many countries, including the United States of America, introduced such measures as pre-flight and luggage controls. Later, the Computer Assisted Passenger Prescreening System (CAPPS) was introduced in the US, which allowed automatically singling out certain passengers and putting them through stricter controls.

After terrorist attacks 11 September 2001 the US intensified collection of passenger data developing the Passenger Name Records (PNR) system, claiming that it would be used for the purpose of combating terrorism and crime only.

On 19 November 2001 the US implemented Aviation and Transportation Security Act, requiring all airlines flying to or from the US to disclose to the US Bureau of Customs and Border Protection (CBP) and the Transportation Security Agency (TSA)[2] personal data contained in PNR of air passengers. According to the Act, the transfers of passenger data must be completed before the plane takes off, or at the latest 15 minutes after departure. Not only the US Customs, but all US federal

[2] According to the US Homeland Security Act of 2002, many of the federal agencies responsible for border and transportation security were consolidated into the Department of Homeland Security (DHS). TSA and CBP are sub-departments of DHS.

agencies can have access to these data. CAPPS was then redesigned into CAPPS II. In 2004, the latter was replaced by the passenger-prescreening scheme Secure Flight, which is designed to compare passenger information against watch lists (so-called "selectee" and "no fly" lists, i.e. lists of individuals who "pose a threat") maintained by the federal government in the Terrorist Screening Database[3]. The goal is "to vet 100 percent of passengers on all domestic commercial flights by early 2010 and 100 percent of passengers on all international commercial flights by the end of 2010"[4].

On 14 May 2002 the US adopted another law to enhance border security that requires airlines arriving and departing from the US to transmit data relating to passengers and crew to US Immigration and Naturalization Service (INS). It provides that all data must be transmitted to a centralized database - Interagency Border Inspection System, which also is shared with other US federal agencies.

Due to the fact that these actions concerned not only American airlines, but airlines worldwide, including European companies, in June 2002 the European Commission expressed to the US its opinion that the established requirements were in conflict with the European Union (EU) and Member States' legislation on data protection, in particular the Directive. The latter, inter alia, prohibits transfer of personal data from EU/EEA[5] to the countries lacking adequate level of protection (Article 25).

Pursuant to Article 25(6) of the Directive, determinations of adequacy which are binding on EU/EEA Member States are made by the European Commission with

---

[3] The Intelligence Reform and Terrorism Prevention Act of 17 December 2004, DHS' Notice of Proposed Rulemaking of 8 August 2007, and Secure Flight Final Rule of 22 October 2008. See also: http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm.

[4] TSA, *TSA's Secure Flight Enters First Public Phase*, http://www.tsa.gov/press/releases/2009/0512.shtm.

[5] The Directive was incorporated on 25.06.1999 into 1992 Agreement on the European Economic Area (EEA). Thus EEA member states which are not members of the EU (Norway, Lichtenstein and Iceland) are legally bound by the Directive.

input from Article 29 Working Party[6], the Article 31 Committee, and the European Parliament[7]. But to date, only a few countries, namely Argentina, Switzerland, Hungary, Guernsey, the Isle of Man and, for certain purposes, Canada[8] have met the criteria.

With reference to the US, there exists the Safe Harbour system, which is considered to provide adequate level of protection[9]. The Safe Harbour principles are intended for use solely by US organizations receiving personal data from the EU for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates[10]. But air passenger data transfer lies outside this system, since, according to Article 29 Working Party Opinion 6/2002, the Safe Harbor principles cannot apply for data transfers to government authorities. Thus, with regards to air passenger data, EU had no grounds to consider US as a country providing an adequate level of protection.

The US then agreed to several postponements of the application of the rules to the airlines established in the EU. From this point, EU and US started negotiations aimed at reaching agreement on sharing air passenger data (demanded by the US) while securing an adequate level of protection (demanded by the EU).

The idea of each airline being able to negotiate a separate compromise with the relevant data protection authority and the US government did not seem to be the most

---

[6] Working Party on the Protection of Individuals with regard to the Processing of Personal Data established pursuant to Article 29 of the Directive (Article 29 Working Party). This organ consists of representatives from each EU Member State's data protection authority. It acts independently of the Commission and other EU organs, but has advisory competence only.

[7] Council Decision 1999/468/EC of 28.6.1999 laying down the procedure for the exercise of implementing powers conferred on the Commission (OJ L 184, 17.7.1999, 23).

[8] See, for example, Commission Decision 2000/519/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary, and other respective Commission decisions.

[9] Commission decision of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (2000/520/EC), OJ L 218 of 25 August 2000.

[10] Safe Harbor Privacy Principles issued by the US Department of Commerce on 21.07.2000, Annex I.

efficient way of dealing with the problem. Moreover, the EU realized the benefit of having a single EU-US agreement rather than 27 bilateral agreements between the EU Member States and the US.

Nevertheless, the CBP announced that from 5 March 2003 all international airlines had to provide the US government full electronic access to detailed airline passenger data on all travellers registered in the airline's computer system. The US threatened airlines that failure to provide the requested data after that date would lead to a fine and, potentially, the withdrawal of their landing authorisation.

European airlines found themselves in a difficult situation: to fly from EU to the US, they would need to comply with either EU or US law, but they could not comply with both. They could either refuse to transmit the data thus becoming subject to US authorities' sanctions, or they could deliver the data violating EU law. Since they were not in the position to just stop flying across the Atlantic, most EU airlines chose to provide PNR to the US[11].

At the same time, intensive negotiations between the European Commission and the Department of Homeland Security (DHS) continued, trying to find a formula that would satisfy the US anti-terrorist requirements and allow the EU to issue an "adequacy finding" in respect of the US data protection provisions.

2.1.2 API and PNR

[11] See: Ioannis Ntouvas, *Air Passenger Data Transfer to the USA: the Decision of the ECJ and latest developments*, International Journal of Law and Information Technology, Vol. 16, Issue 1, pp. 73-95, 2008.

First of all, we would like to define what actually the subject of the problem is. What is supposed to be meant by “personal data” in respect of the air passengers travelling across the Atlantic?

Currently, within the US requirements, airlines must transmit two types of passenger data to the US authorities: (i) passenger manifest, or, in other words, Advanced Passenger Information (API); and (ii) Passenger Name Record (PNR).

API system (APIS) is a unilateral system whereby required data elements are collected and transmitted to border control agencies prior to flight arrival, and made available on the primary line at the port of entry[12].

The collection, storage, and forwarding of API data (unlike PNR data) serve no business purpose for airlines. It is solely a passenger surveillance and immigration law enforcement function carried out by the airlines on behalf of governments.

The first international Guidelines on Advance Passenger Information were adopted in 1993 by the World Customs Organization (WCO) and International Air Transportation Association (IATA). These Guidelines limited data requirements to the minimum required to conduct pre-arrival checks and to those data elements found in the machine readable zone of travel documents. After 11 September 2001, WCO and IATA, joined by the International Civil Aviation Organization (ICAO), revised the Guidelines.

The new Guidelines were released in June 2003. To ensure the Guidelines continue to hold their relevance, WCO established API Management Committee, which is tasked with the ongoing review of the Guidelines and an effort to promote the Guidelines'

[12] Advanced Passenger Information – A Statement of Principles, Cairo, Egypt, ICAO, 12th Session, 22 March to 2 April 2004.
http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp060_en.pdf.

global adoption. But the requirement that the API elements should be limited is still valid: "Required API data should be limited to the data contained in the machine-readable zone of travel documents or obtainable from existing government databases, such as those containing visa issuance information."[13]

The Guidelines have been used as the basis for API formats for messages between airlines and Computerized Reservation Systems (CRS). But they still have not been agreed to by all governments that have, or are considering, API requirements.

At first, the US demands for API were limited. But currently, the US authorities request as follows:

- name
- date of birth
- gender
- citizenship
- country of residence
- travel document type, its number, expiration date, country of issuance
- foreign registration number (if applicable)
- address while in the US
- passenger contact information (phone)
- any other data deemed necessary to identify the persons traveling[14].

Demands for the additional information, such as passenger addresses and phone numbers, along with the above-mentioned Secure Flight program requirements, exceed the Guidelines' recommendations.

---

[13] See *supra* n.12.

[14] See: CBP's Message Implementation Guideline for Airlines of 23 February 2009; Final Rule on Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels. DHS, CBP, 23 August 2007. 19 CFR Parts 4 and 122 [USCBP–2005–0003; CBP Dec. 07–64] RIN 1651–AA62.

In 2003, in the comments submitted to the US government, IATA stated that "the most critical and problematic is the expanded list of required data elements."[15] Moreover, according to IATA, the actual costs for both the program's initial implementation and data collection and airport operations will rise significantly higher than the estimated cost of $164 million, which is "a staggering financial imposition for an industry."[16]

"The Passenger Name Record (PNR) is the generic name given to the files created by the airlines for each journey any passenger books. They are stored in the airlines' reservation and departure control databases. PNR allows all the different agents within the air industry (from the travel agent and the computer reservation systems (CRS) to the carrier and the handling agents at the airports) to recognise each passenger and have access to all relevant information related to his/her journey: departure and return flights, connecting flights (if any), special services required on board the flight, etc. The number and nature of fields of information in a PNR system will vary from airline to airline. There are approximately 20-25 possible fields of PNR data, some of which include subsets of information, expanding the total to approximately 60 fields and sub-fields"[17].

A PNR is the basic form of computerized travel record[18], and, by contrast with API, includes data from which aspects of the passenger's history, conduct and behaviour can be deduced. Most airlines store PNR in the database of a Computerized Reservation System. The PNR system contains all passenger data of the whole airline company, thus, the system is not restricted to a specific flight and allowing full access

[15] Comments of the IATA in respect of: US Immigration and Naturalization Service Notice of Proposed Rulemaking on Manifest Requirements Under Section 231 of the Act 8 CFR Parts 217, 231 and 251 RIN 1115-AG57 (Federal Register/ Vol. 68, No. 2, 03 January 2003) of 3 February 2003.
[16] See *supra* n.15.
[17] Airlines passenger data transfer from the EU to the United States (Passenger Name Record) – frequently asked questions. Memo/03/53. Brussels, 12 March 2003.
[18] Example of PNR: http://www.amadeusuk.com/Training/TrnPNRCheat.htm

to the departure control systems and PNR means that the US agencies also get full access to data of passengers who do not fly to the US at all.

A PNR is created every time a traveller makes a reservation. PNR cannot be deleted: once created, they are archived and retained in CRS, and can still be viewed, even if a person never bought a ticket or cancelled the reservation. Each entry in each PNR, even for a solo traveller, contains identifiable information on at least two, often more, people: the traveller, the travel arranger or requester, the travel agent or airline staff person, and the person paying for the ticket.

Most travel agencies also use the CRS as their primary customer database and accounting system and store all customer data in CRS profiles. Thus PNR also contain data on individuals who never travel by air at all, since lots of travel services, car rental and hotel reservations, etc, made through travel agencies, are made through CRS. PNR provides a comprehensive and extremely detailed record of every entry and show what was entered, when, where, by whom, for whom, where you went, who went, when, with whom, for how long, and at whose expense. Through special service codes, PRN reveal details of travellers' physical and medical conditions. For instance, through special meal requests, they contain indications of travellers' religious practices, i.e. a category of data typically referred to “sensitive information”.

There are four major CRS in the world; Amadeus is the only one of them based in the EU rather than the US. Each of them has a web site that gives anyone access to PNR data, very often with no password at all, just the reservation number printed on every ticket.

“But with CAPPS-II and Secure Flight, you need to know: PNR's are the records about each airline passenger that are being used USA government's Secure Flight (formerly named ‘CAPPS-II’) passenger surveillance and permission system and ‘no-

fly' lists, and compiled into the Automated Targeting System (ATS) and other databases of the Transportation Security Agency (TSA) and Customs and Border Protection (CBP) divisions of the Department of Homeland Security (DHS)."[19]

There appear some financial concerns as well. Up to date, according to IATA, the cost of transferring API to authorities is approximately US$14 per flight or more than US$100 million annually[20]. Providing the PNR data in addition to API would make the expenses, as well as the above-mentioned amount of $164 million, even more. Apparently, these costs, imposed on the airlines and other agents within the air industry, would ultimately have to be borne by travellers.

2.1.3 Data Protection Directive v. US Law

In order to understand what actually constitutes the problem of the EU-US data transfer from legal point of view, it is necessary to analyze the applicable legal instruments in more detail.

The right to privacy is protected by the following international instruments:

- the Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.01.1981. This Convention is not self-executing: it obliges members of CoE to incorporate its principles into their national legislation. It is open for ratification by states other than members of CoE (the US never ratified it);
- the Directive 95/46/EC (it is binding for EU/EEA member states);

[19] Edward Hasbrouck, *What's in a Passenger Name Record (PNR)?* http://hasbrouck.org/articles/PNR.html
[20] http://www.iata.org/pressroom/facts_figures/fact_sheets/security.htm

- the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23.09.1980. They were adopted in the form of recommendations and are not legally binding on OECD members (including the US);
- United Nations Guidelines Concerning Computerized Personal Data Files of 14.12.1990 (not legally binding).

In addition, the privacy right is protected by Article 8 of the European Convention on Human Rights (ECHR) as well as being enshrined in Article 7 and 8 of the Charter of Fundamental Rights of the European Union (both applicable in the EU).

The US therefore is not legally bound by any of the above-mentioned documents. In fact, "a major formal aim of international data protection instruments is to stimulate the creation of adequate national data protection regimes and to prevent divergence between them"[21]. The Directive is the most comprehensive of the instruments. It is based on the principles established by the other mentioned documents and actually constitutes the most important point of departure for new data protection initiatives, both in and outside the EU[22]. Thus the Directive will be analyzed as the principal source of the EU data protection legislation.

The Directive's aim is harmonization of national data protection regimes (recital 8) and it requires EU Member States to create legislation implementing the provisions of the Directive. In addition, the European Parliament and European Council established the European Data Protection Supervisor (EDPS), which is an independent supervisory authority that regulates the processing of data.

The Directive applies to the processing of personal data. While the terms "personal data" and "processing of personal data" are defined in Article 2 of the Directive,

[21] See: Bygrave, Lee A. *supra* n.1.
[22] See: Bygrave, Lee A. *supra* n.1.

Article 6 provides for strict requirements to data processing: personal data must be (i) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (ii) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (iii) accurate, relevant, kept up to date; and (iv) stored only as long it is necessary for the given purpose. Moreover, there are other requirements such as the data subject's right to be informed of the data processed, purposes of such processing, *etc*. (Articles 10 and 11), and the right of access (Article 12).

The Directive provides exemptions in Article 13, which stipulates that the Member States may restrict the scope of the obligations and rights mentioned above when such a restriction constitutes a necessary measure to safeguard, inter alia, national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences. But this article cannot be applicable to the US request, since the indication of "necessary measure" explicitly means that these exemptions are restricted only for specific investigations, a case by case request, and not to the case where the personal data transfer is systematic as it is foreseen by the US Customs[23].

The US requests for data access are in conflict with the above-mentioned principles of Article 6, specifically, with the requirement that the data controller can process personal data only if processing is compatible with the original purposes of data collection. Transfer of passenger personal data by airlines to the US government agencies can hardly be seen as fulfillment of airlines' contractual obligations towards their passengers, i.e. provision of definite services. The airlines did not originally intend to collect data to transfer them to the US Customs (although one may argue that without such transmission airlines would fail to carry their passenger to the US).

[23] Electronic Privacy Information Center, EU-US Airline Passenger Data Disclosure, available at: http://www.epic.org/privacy/intl/passenger_data.html (detailed history of PNR data conflict).

Another problem already mentioned in 2.1.1 is that Article 25 provides that personal data may only be transferred to third countries (i.e. non-EEA countries) if the specific country ensures an adequate level of protection. The Safe Harbour system, which is construed to provide adequate protection, is not applicable for the EU-US air passenger data transfer. Thus there should be established additional guarantees, which could constitute adequate protection. But what actually is meant under "adequate protection"?

The purpose of data protection is to afford protection to the individual about whom data are processed. This is typically achieved through a combination of rights for the data subject and obligations on those who process data, or who exercise control over such processing. Analysis of adequate protection must comprise the two basic elements: the content of the rules applicable and the means for ensuring their effective application. Using Directive as a starting point, and bearing in mind the provisions of other international data protection texts, it should be possible to arrive at a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate.[24]

Protection afforded by the US law[25] is very different to that provided by the Directive. While the EU has historically enacted broad legislative protection of personal data, the US has promoted the self-regulation of industries through the use of broad reaching legislation[26]. Nevertheless the US Constitution and interpreting case

[24] Article 29 Working Party, Opinion 12/98, 24.07.1998, Transfers of personal data to third countries. Applying Articles 25 and 26 of the EU Data Protection Directive.
[25] See, for example: Privacy Act of 1974, Freedom of Information Act and the E-Government Act of 2002, Aviation Transportation Security Act of 2001, the Homeland Security Act of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004 and Executive Order 13388 regarding cooperation between agencies of the United States government in combating terrorism.
[26] Megan Roos, *Safe on the Ground, Exposed in the Sky: The Battle Between the United States and the European Union Over Passenger Name Information*, 14 Transnat'l L. & Contemp. Probs. 1137, 1154-55, 1161 (2005); John B. Reynolds, III, *View from Washington, European Union (EU) Privacy Directive Enters Into Force*, archived at http://www.webcitation.org/5WBIN8Xwm.

law does provide some protection of an individual's privacy, however, this is a general protection and courts have not yet interpreted the Constitution broadly enough to include a protection of information privacy from government misuse[27]. Despite this lack of overarching protection, there are some statutes that limit the use of data, using the aforementioned sectoral approach, for example, the Privacy Act of 1974.

But the Privacy Act only protects personal information when it is processed by the federal government. The US has no general law protecting the privacy of "commercial" data. Thus PNR data has been considered the "property" of airlines, CRS and other travel companies, over which travellers have no control. Those travel companies could allow the US government agencies to look at PNR without the knowledge or consent of the data subjects. There is no comparable privacy law requiring disclosure to passengers of how their travel records are used. Thus, even brief analysis of the US law leads to the conclusion that afforded protection cannot be considered as "adequate".

Article 26 of the Directive stipulates that transfer of personal data to a country which does not ensure an adequate level of protection on condition that data subject (in our case, a passenger) has given his consent unambiguously to the proposed transfer. This means, pursuant to the Directive, a "freely given specific and informed indication of a person's wish." According to Articles 10 und 11 of the Directive, the information provided to the data subject must include the identity of the US Agency, the purpose of this request and a notification that the data will be transferred to a country that does not offer adequate privacy safeguards.

---

[27] Arnulf S. Gubitz, *The U.S. Aviation and Transportation Security Act of 2001 in Conflict With the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?*, New England Las Review, volume 39 (2005) 446-447.

Nevertheless, in his speech on 16 December 2003, Frits Bolkestein, Member of the European Commission, stated the following with reference to this exemption: "Simply by telling the airlines that they had to obtain the unambiguous consent of all passengers, we could have solved the problem. This regardless of whether protection in the US was adequate or not, because consent allows you to make an exception. Indeed this way, we could have solved most of the legal problems. And the underlying proposition that people must be informed and have the opportunity to make a choice is certainly a very valid one that the Commission fully supports. But relying on consent alone would have been bad data protection, even if it resolved the legal problems. We would have been saying to people: it is up to you to decide whether to go to the US, but we are washing our hands entirely of what happens to your personal data once it gets to the US." [28]

But even if we imagine that the Commission would follow the "bad data protection" scheme described above, there are still doubts whether such passenger's consent would be relevant under the Directive, since it would not have been given "freely", as long as the consequence would be a denial of travelling.

The other exemptions listed in Article 26 do not apply. There is neither a proof that the transmission of the specific data is necessary to safeguarding important public interests, nor that the transmission is necessary in order to protect the vital interests of the passengers.

National law of EU/EEA Member States, which derives from the Directive, also forbids or limits the possibility of data transfers to third countries, inasmuch as they do not guarantee an adequate level of data protection.

---

[28] Speech/03/613 addressed to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market, Strasbourg, 16 December 2003. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/03/613&format=HTML&aged=1&language=EN&guiLanguage=en

But the problem of the US' lack of adequate level of protection could be resolved by another method, namely, by concluding an agreement, where adequate safeguards could be provided.

According to Article 29 Working Party Opinion 12/98 of 24.07.1998, for a contractual provision to provide adequate safeguards, it must satisfactorily compensate for the absence of a general level of adequate protection by including the essential elements of protection which are missing in the particular situation. The basis for assessing the adequacy of the safeguards delivered by a contractual solution is the same as the basis for assessing the general level of adequacy in a third country. The specific requirements of a contractual solution are as follows:

(i) The substantive data protection rules:

- the purpose limitation principle
- the data quality and proportionality principle
- the transparency principle
- the security principle
- the rights of access, rectification and opposition
- restrictions on onward transfers to non-parties to the contract.

In some situations additional principles relating to sensitive data, direct marketing and automated decisions must be applied. The contract should set out the detailed way in which the recipient of the data transfer should apply these principles (i.e. purposes should be specified, data categories, time limits for retention, security measures, etc.). Detail is imperative where the transfer is based on a contract.

(ii) Rendering the substantive rules effective:

- to deliver a good level of compliance with the rules

- to provide support and help to individual data subjects in the exercise of their rights
- to provide appropriate redress to the injured party where rules are not complied with.

But was it possible for the parties to reach such an agreement? Was the US in the position to provide data protection guarantees which would satisfy to such requirements?

2.2 Solution: PNR Agreement

2.2.1 PNR Agreement 2004

The difficult situation described in section 2.1.1 led the EU institutions to explore the possibility of a political resolution of the conflict. Negotiations continued. The discussions essentially sought to enhance US data protection standards and reduce those of the EU. The intention was to conclude a bilateral EU-US agreement, which would allow the Council of Europe to permit CBP to receive personal data from EU airlines and at the same time would oblige CBP to provide certain data protection guarantees when processing these data. Such guarantees should be considered as providing an adequate level of data protection in the framework of Data Protection Directive Article 25(2).

But the negotiations were tricky. In particular, the US refused to limit access to the data to agencies seeking to combat terrorism. There were also difficulties over the length of time the data should be kept. The EU expected the data to be retained for a period of weeks or months, while the US wanted to keep it for fifty years.

Finally, in December 2003, the Commission announced that it had reached agreement with the US[29]. The main points of the deal were as follows:

1) the US could access 34 different types of personal data (the full list is available in Annex 3 hereto) under a so-called "pull" scheme. This means that the US could access the data in CRS directly instead of having the information transferred and possibly filtered, anonymised or pseudonominised (so-called "push" scheme). The distinction between "pull" or "push" system is crucial. In the context of Directive

[29] See: Letter from Commissioner Bolkestein to US Secretary Tom Ridge, Department of Homeland Security, 18.12.2003.

Articles 25 and 26, one must differentiate between a recipient and a sender. The latter can only be the controller[30] of the processing operation in the sense of Directive Article 2(d), who therefore is bound by Article 25. The nature of the person, who does not receive data, but has access thereto in the sense of Article 4(1)(c), is rather a controller (of a second processing operation, separate from the initial). CBP accessing PNR data through a "push" system makes it a recipient, whereas a "pull" system makes it a controller, to which the Directive is applicable. CBP could be seen as a controller even in the context of a "push" system, if one assumes that the purposes of combating and preventing terrorism and other serious crimes diverge so significantly from the initial purpose of processing, that they should be considered as a processing operation banned under Article 6(1)(b). Processing by CBP would then count as a new, separate set of processing, thus require a legal basis from Article 5[31];

2) the US shall store the data for 3,5 years and, in certain cases, much longer;

3) the arrangement shall not cover CAPPS II;

4) the US accepted after refusing it earlier a safeguard in the form of a joint review, to be carried out together with EU authorities at least every year;

5) acceptance of redress for individual EU passengers: the US recognized the right of EU data protection authorities to represent EU citizens (passengers whose complaints to the DHS have not been satisfactorily resolved by the DHS or its Privacy Office);

6) all categories of sensitive data will be deleted;

7) a set of processing purposes was reduced from 'any purpose' to 'combating serious crime and terrorism';

8) the US promised to use data only within the DHS and not to pass it on to other agencies.

---

[30] Under the Directive the 'controller' must take the principal responsibility for complying with the substantive data protection principles. The 'processor' is responsible only for data security. An entity is deemed to be a controller if it has the decision-making power over the purposes and means of the data processing, whereas the processor is simply the body that physically provides the data processing service. See Article 29 Working Party Opinion 12/98, 24.07.1998.

[31] See: Ioannis Ntouvas, *supra* n 11.

The deal received substantial criticism from different institutions. The Article 29 Working Party issued its Opinions in October 2002 (Opinion 6/2002), on 13 June 2003 (Opinion 4/2003), and finally on 29 January 2004 (Opinion 2/2004)[32]. In the latter, it was stated that the transfer of data to US authorities raised public concern and had broad and sensitive implications in political and institutional terms, as well as having an international dimension. The following outstanding points were indicated:

1) Data quality:

- the purposes of the data transfer should be limited to fighting acts of terrorism and specific terrorism-related crimes to be defined;
- the list of data elements to be transferred should be proportionate and not excessive;
- data matching against suspects should be performed according to high quality standards with a view to certainty of the results;
- the data retention periods should be short and proportionate;
- passengers' data should not be used for implementing and testing CAPPS II or similar systems.

2) Sensitive data should not be transmitted.

3) Data subjects' rights:

- clear, timely and comprehensive information should be provided to the passengers;
- rights of access and rectification should be guaranteed on a non discriminatory basis;
- there should be sufficient guarantee that passengers would have access to a truly independent redress mechanism.

4) Level of commitments by US authorities:

[32] Article 29 Working Party, Opinion 2/2004 of 29.01.2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection.

- the US commitments should be fully legally binding on the US side;
- the scope and legal basis and value of a possible "light international agreement" should be clarified.

5) Onward transfers of passenger PNR data to other government or foreign authorities should be strictly limited.

6) Method of transfer: a "push" method of transfer, whereby the data are selected and transferred directly by airlines to US authorities, should be put in place.

In February 2004 Privacy International[33], in association with European civil rights groups Statewatch[34] and the European Digital Rights Initiative (EDRI)[35], published a report - scathing attack on the deal[36]. The report illustrated the results of the negotiations in the table which is Annex 2 hereto. In summary the report alleges:

- DHS gets access to EU airline database records even though the DHS does not require similar access to US carriers' computer systems and records.
- The US now has data to test and implement its controversial CAPPS II, using European passenger data instead of American passenger data. The European Commission believes that the DHS will remove this data once testing is complete. This is an unacceptable risk taken by the Commission.
- The European Commission is now speaking of creating a centralised database of all passenger records so that the records can then be transferred to the US, creating further privacy and security concerns.

---

[33] Privacy International is a private human rights advocacy group formed in 1990 "as a watchdog on surveillance and privacy invasions by governments and corporations". http://www.privacyinternational.org

[34] Statewatch is a non-profit-making voluntary group founded in 1991. It is comprised of lawyers, academics, journalists, researchers and community activists. http://www.statewatch.org

[35] EDRI was founded in June 2002. Currently 28 privacy and civil rights organisations have EDRI membership. http://www.edri.org

[36] First Report on "Towards an International Infrastructure for Surveillance of Movement". Privacy International, in co-operation with European Digital Rights Initiative, the Foundation for Information Policy Research, and Statewatch, with a Commentary from the American Civil Liberties Union on A Perspective from America, February 2004.

- The European Commission wishes to see the development of EU-based laws that will grant database access to EU member states for law enforcement purposes. The EU also wishes for access to US passenger data, but has not yet negotiated this with the Americans.
- After establishing European surveillance laws, the European Commission is also seeking to create a global regime on passenger records surveillance through the UN agency, the ICAO, thus permitting all countries to gain access to this data.

Members of European Parliament (MEPs) in the EP Citizens' Rights Committee also strongly criticised the Agreement. On 17 March 2004 they adopted a resolution opposing the transfer of personal passenger data to US. In particular, they objected to:

- the number of PNR items (34) the US wants to obtain;
- the purposes for which the data might be used (not only for fighting terrorism, but also for fighting "serious crime");
- the lack of redress mechanisms for people who are denied entry to the US on the basis of the information in the PNR records;
- the lack of opportunities for passengers to correct errors in their personal data;
- the fact that a "pull" instead of a "push" system is used to obtain the data, meaning that the US does not have to ask for the data but has immediate access to it;
- the number and kind of agencies that have access to the personal data.

On 11 May 2004 the CBP released its PNR Undertakings (Undertakings), based on the result of the agreement with the EC in December 2003[37].

Despite the above-mentioned objections, the Commission found the agreement adequate[38]. On 17 May 2004, the Council adopted a decision approving the

[37] Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data, 69 Fed. Reg. 41543-41547, 9 July 2004.

conclusion of the agreement. The Agreement between the European Community and the USA on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security and Bureau of Customs and Border Protection was signed and entered into force on 28 May 2004 (PNR Agreement 2004). Notably, the most essential terms and conditions of the deal were contained in the Undertakings, which the Agreement only referred to.

But one of the key problems was that neither the PNR Agreement 2004, nor the Undertakings had any legal force or effect in the US.

With regards to the Undertakings, on the one hand, CBP was bound by them in the sense that "CBP takes note of the Decision and states that it is implementing the Undertakings annexed thereto" (PNR Agreement 2004, Paragraph 3) and that CBP "will issue regulations, directives or other policy documents incorporating the statements herein, to ensure compliance with these Undertakings by CBP officers, employees and contractors […] failure to abide […] may result in strict disciplinary measures being taken, and criminal sanctions, as applicable" (Undertakings, Paragraph 44). From the other hand, "These Undertakings do not create or confer any right or benefit on any person or party, private or public" (Undertakings, Paragraph 47). Moreover, as of publication, the Undertakings did not take statutory form in the US. To this extent it was questionable if anything, apart from diplomatic considerations, could prevent CBP or other US authorities processing PNR data from not complying with the Undertakings[39].

[38] Commission decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (2004/535/EC), OJ L 235 of 6 July 2004.
[39] See: Ioannis Ntouvas, *supra* n 11.

With regards to the PNR Agreement 2004, to be binding and enforceable on the US, an international agreement must be signed by the President, and ratified by the Senate as a treaty, or be enacted into US law. Nothing of this was done.

The question of the Agreement's validity in the EU will be considered in detail in section 2.2.2. According to the European Court of Justice, the Council was not entitled to conclude the agreement with the US in the name of the European Community (EC). Therefore, the Agreement was annulled and was not binding on the EU.

Another question is whether the Agreement was binding on the EU Member States. Even if the Agreement were valid, could Member States be affected by such an act, and would their national law thus be altered to permit the data transfer?

Ministers of foreign affairs of Member States are, as a general rule, authorised to conclude international agreements. The Council consisted, at the moment of conclusion of the Agreement, of said ministers. Even if they, acting collectively, did not act as an EC instance (lacking a legal basis in the EC Treaty), each foreign minister could conclude acts binding upon his own state. The agreement can thus be seen as an aggregation of bilateral international treaties between each EC member state and the US. In particular, the Council did not act as such, but reached a decision as a governmental conference. Thus, the Agreement binds Member States; the question remains, however, if it changes their legal systems. Typically, in order to be incorporated into national law, international treaties must be ratified by Parliament. Before such ratification the PNR transfer is still governed only by national law and is generally prohibited. This prohibition can evidently not be limited by Article 8 of the PNR Agreement 2004 stipulating that "This Agreement is not intended to derogate

from or amend legislation of the Parties; nor does this Agreement create or confer any right or benefit on any other person or entity, private or public."[40]

Annulled by the Court, the Agreement could not therefore be invoked to justify the data transfer. But even if it were valid, could it legalise the PNR transfer on the grounds that it provided an adequate level of data protection?

The Commission found the Agreement adequate, but Article 29 Working Party, MEPs and privacy advocates insisted on the opposite.

The "weakest points" of the Agreement contravened to the above-mentioned requirements of a contractual solution determined by Article 29 Working Party Opinion 12/98 pursuant to the Directive. It concerned both the substantive data protection rules and requirements for making them effective.

Specifically, the purposes for which the data might be used did not satisfy to the purpose limitation principle. The "detail" requirement was not followed, especially concerning data quality and data subjects' rights. The Agreement suffered the lack of mechanisms for (i) redress, access and rectification, and (ii) provision of information to the passengers. Sensitive data, which should not be transmitted, could be submitted in some cases. A "pull" instead of a "push" system was used.

Furthermore, the US promised that the arrangement would not cover CAPPS II, but later, the US confirmed that the PNR data would be used for testing CAPPS II[41]. The US promised not to pass the data to other agencies. There was, however, no verification mechanism for this promise, neither was there one for the deletion of the

---

[40] See: Ioannis Ntouvas, *supra* n 11.
[41] See, for example, Answer given by Mr Bolkestein on behalf of the Commission, 11 March 2004. OJ 84 E/167, 3.4.2004.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:084E:0166:0167:EN:PDF

data at the end of the agreed storage period. The "joint review" procedure was not clearly specified in the Agreement thus it could hardly be considered as such verification mechanism.

But, as we can see, despite these facts, the Commission argued that the Agreement was adequate. The criticisms were consistent, culminating in a vote by MEPs to refer the agreement to the court for an opinion.

2.2.2 European Court of Justice Decision

On 27 July 2004 the EP brought action before the European Court of Justice (ECJ) against the Commission's decision on adequacy and the Council's decision adopting the PNR Agreement 2004, on the grounds that they did not comply with provisions of the Directive and ECHR Article 8. EP accused the Commission of misuse of powers, breach of fundamental rights and of the principle of proportionality.

The ECJ ruled, on 30 May 2006, that neither the Commission decision finding that the data were adequately protected by the US nor the Council decision approving the conclusion of an agreement on their transfer to that country were founded on an appropriate legal basis. [42]

The Directive does not apply to activities which fall outside the scope of Community law such as public security, defense, and state security (Article 3). So while the Commission was arguing that the PNR Agreement 2004 was permissible under the Directive (and thus adequate), the decision was also about whether the Commission

[42] Judgment of the European Court of Justice in Joined Cases C-317/04 and C-318/04, European Parliament v. Council of the European Union and European Parliament v. Commission of the European Communities, 30 May 2006.

had sufficient jurisdiction to create an agreement on that basis with the US on such matters.

The ECJ found that "Article 95 EC, read in conjunction with Article 25 of the Directive, cannot justify Community competence to conclude the Agreement. The Agreement relates to the same transfer of data as the decision on adequacy and therefore to data processing operations which, as has been stated above, are excluded from the scope of the Directive. Consequently, Decision 2004/496 cannot have been validly adopted on the basis of Article 95 EC. That decision must therefore be annulled and it is not necessary to consider the other pleas relied upon by the Parliament" (Para. 67-70).

To explain the Court's logic, we must remind that the EU has a complicated constitutional structure. It has three "Pillars." The First Pillar governs the regulation of the common market, where the EU has acquired a lot of power, and the Member States have lost a lot of power. The Second and the Third Pillars apply to defense and other types of foreign policy (Second Pillar) and fighting crime and protecting against internal security threats like terrorism (Third Pillar). The EU has powers in these areas, but it is limited by Member States preserving national sovereignty.

Since the PNR agreement involved private commercial carriers, the European institutions acted under the First Pillar: the Commission based its decision on the Directive (a market-regulating, First Pillar law) and the Council based its decision on the Directive, together with its more general First Pillar powers.

But the ECJ eventually considered that the EU would have to act under the Third Pillar or not at all. The Court, in its own analysis, put the transfer of PNR data squarely in the Third Pillar: the Court stated, without reservation that the data transfer covered by that agreement was "not data processing necessary for a supply of

services, but data processing regarded as necessary for safeguarding public security and for law enforcement purposes." (Para. 57)[43].

As a result, the ECJ annulled both the Commission and Council decisions and obliged the Council to terminate the agreement. Data transfers would continue during a transition period until 30 September 2006, after which the ECJ judgment would take effect. But the ECJ did not consider the privacy and human rights aspects of the PNR Agreement 2004, including the conformity of the PNR regime with provisions of the Directive. Thus it did not settle the matter.

2.2.3 Interim Agreement 2006

After the decision of the ECJ, mindful of the potential legal uncertainty for European airlines operating transatlantic services, the Commission and the EU's presidency were promptly mandated by the Council to resolve the situation by means of a new agreement. Another round of negotiations began.

US Secretary of Homeland Security, Michael Chertoff, repeatedly stated that the current scheme for transferring European air passenger data to US authorities was insufficient to fight terrorism. He demanded for more of the detailed information collected by airlines and travel agencies when a person books a flight, including phone numbers used for booking a flight, as well as travel itineraries and payment details. He also asked authorisation for the CBP, which received the data, to share it with Immigration and Customs Enforcement and with the FBI[44].

---

[43] Francesca Bignami, *European Court of Justice Strikes EU-US Agreement on PNR Data*, 31 May 2006. http://www.concurringopinions.com/archives/2006/05/european_court.html.
[44] Michael Chertoff, *A Tool We Need to Stop the Next Airliner Plot*, Washington Post, 29.08.2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/08/28/AR2006082800849.html

European Commissioner for Justice, Freedom and Security Franco Frattini said that he "will try to renegotiate the current PNR agreement under different legal basis, but with similar content."[45]

On 6 October 2006, an "Interim Agreement"[46] was signed, with validity until 31 July 2007. Since the previous agreement was in effect until 30 September 2006 (pursuant to the ECJ's decision), the Interim Agreement ended a week of legal limbo for airlines. It was substantially similar in content to the PNR Agreement 2004 but on a different legal basis (Third pillar).

Instead of "European Community", "European Union" was indicated as the contracting party. With regards to the "European Union", we must note here that the EU Treaty does not contain any provisions on the Union's legal personality even though the Union comprises the two Communities (European Community and European Atomic Energy Community) and two areas of intergovernmental cooperation, namely common foreign and security policy (CFSP) and police and judicial cooperation in criminal matters. The question of the Union's legal personality has essentially been raised in connection with international relations, especially the power to conclude treaties or accede to agreements or conventions. The Union does not have institutionalised treaty-making powers, i.e. international capacity to enter into agreements with non-member countries. However, it pursues its own objectives at international level, whether by concluding agreements through the Council of the European Union or by asserting its position on the international stage, especially in connection with CFSP[47].

---

[45] EurActiv.com, *ECJ puts end to EU air passenger data transfers to US*, 31 May 2006. http://www.euractiv.com/en/security/ecj-puts-eu-air-passenger-data-transfers-us/article-155680

[46] Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, 2006 O.J. (L 298) 29.

[47] See: http://europa.eu/scadplus/glossary/union_legal_personality_en.htm

Although the Agreement did not mention its legal base, it was understood that this was provided by EU Treaty Articles 24 and 38. The Council thus avoided the possibility of EP to bring action against it (EP cannot control acts of the Council taken under non-EC EU law; in this case, in the field of police and judicial cooperation). Furthermore, the problem of national Member State data protection legislation, as described above in 2.2.1, remained.

The Interim Agreement referred to the Undertakings of 2004, which still contained substantial part of the deal (the legal effect of the Undertakings has been discussed earlier. This Agreement was neither enacted into US law nor ratified, thus was not binding for the US). In addition, there appeared another document, not mentioned in the Agreement, in the form of a letter from the DHS to the Commission, which interpreted certain provisions of the Undertakings (DHS Letter).[48] Although published in the Official Journal of the EU, this letter could hardly have formal legal effect.

The Interim Agreement, along with the DHS Letter, introduced, inter alia, the new approaches to the following principles:

1) Availability of information:
The "pull" system will be substantiated by the "push" system. Specifically, the Interim Agreement Paragraph 2 provides: "DHS will electronically access the PNR data from air carriers' reservation systems located within the territory of the Member States of the European Union until there is a satisfactory system in place allowing for transmission of such data by the air carriers." DHS Letter states that "DHS will move as soon as practicable to a push system for the transfer of PNR data in accordance

[48] Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the undertakings issued by DHS on 11 May 2004 in connection with the transfer by air carriers of passenger name record (PNR) data. 27.10.2006. OJ 2006/C 259/01.

with the Undertakings and will carry out no later than the end of 2006 the necessary tests [...] In order to avoid prejudging the possible future needs of the system any filters employed in a push system, and the design of the system itself must permit any PNR data in the airline reservation or departure control systems to be pushed to DHS in exceptional circumstances [...] While Paragraph 14 limits the number of times PNR can be pulled, the provision puts no such restriction on the "pushing" of data to DHS. The push system does not confer on airlines any discretion to decide when, how or what data to push, however. That decision is conferred on DHS by U.S. law. Therefore, it is understood that DHS will utilize a method of pushing the necessary PNR data that meets the agency's needs for effective risk assessment".

2) Comparable standards of data protection:

"The DHS will be allowed to share (without providing unconditional direct electronic access) PNR data freely with other US government authorities exercising a counter-terrorism function that need PNR for the purpose of preventing or combating terrorism and related crimes in cases (including threats, flights, individuals, and routes of concern) that they are examining or investigating. DHS will ensure that such authorities respect comparable standards of data protection to that applicable to DHS, in particular in relation to purpose limitation, data retention, further disclosure, awareness and training, security standards and sanctions for abuse, and procedures for information, complaints and rectification" (DHS Letter).

3) Data retention:

"Several important uses for PNR data help to identify potential terrorists; even data that is more than 3.5 years old can be crucial in identifying links among terrorism suspects. The questions of whether and when to destroy PNR data collected in accordance with the Undertakings will be addressed by the US and the EU as part of future discussions" (DHS Letter).

4) Data elements:

"The Undertakings authorize DHS to add data elements to the 34 previously set forth in Attachment "A" of the Undertakings, if such data is necessary to fulfill the purposes set forth in paragraph 3" (DHS Letter).

5) The Joint Review:

"Given the extensive joint analysis of the Undertakings conducted in September 2005 and the expiration of the agreement prior to the next Joint Review, the question of how and whether to conduct a joint review in 2007 will be addressed during the discussions regarding a future agreement" (DHS Letter).

Analyzing the texts of the Agreement, Undertakings and the DHS Letter, it can be assumed that the scope of the agreement has been widened substantially:

- more data requested
- considerable weakening the purpose limitation
- sharing with more and unspecified agencies
- undefined retention periods
- allowing for more frequent and earlier pushing of data
- no guarantees for a definitive switch to the "push" system
- the virtual abolition of the joint evaluation
- unclear protection of personal data of EU citizens
- unclear means of legal redress.

Thus, in comparison with the earlier PNR Agreement 2004, the new deal looks weaker with reference to the passenger data protection level. The Interim Agreement received much of the same criticism as the previous agreement and undoubtedly needed further negotiations and revisions.

2.2.4 Towards 2007 PNR Agreement

Since the Interim Agreement was supposed to be valid until 31 July 2007 only, discussions and preparatory work for a new long-term agreement proceeded.

In the beginning of 2007, Article 29 Working Party issued two important papers. In the first one dated 10 January 2007 it adopted a standard application for the approval of Binding Corporate Rules (BCR) for multinationals wishing to transfer EU residents' personal data to non-"certified" third countries, such as the US. Specifically, the Working Party's creation of a standard application and clarification of the requirements for BCR certification could represent a small step towards easing the process's procedural burdens. But the Working Party still has not addressed significant substantive issues, such as requirements that could conflict with the national laws of non-member states. Thus, only a handful of companies may find the BCR certification process's intrusive and procedurally complex requirements to be the preferred means of complying with EU privacy regulations.

In the second paper[49], the Working Party clarified its position on various parties' responsibilities stemming from DHS demand for PNR for all inbound international flights. The Working Party required the airlines to tell passengers that information about their travel will be transferred to DHS. The Working Party addressed the proper means of giving notice of PNR transfer to DHS to passengers who book their own

[49] Article 29 Working Party, Opinion 2/2007 of 15.02.2007 on information to passengers about transfer of PNR data to US authorities.

flights on the carrier's website. It advised that the notice must be “presented to passengers automatically, without requiring them to look for it” and then suggested that airlines use pop-up windows as one means of providing the requisite notice. But the Working Party gave no guidance on whether it will deem notice to have been given if a passenger uses pop-up blocking software.

On 26 March 2007 a public seminar by the EP Committee on Civil Liberties, Justice and Home Affairs (LIBE) on transfers of personal data to the US and a preparatory PNR workshop of the Article 29 Data Protection Working Party on the EU approach to a new PNR agreement with the US were held in Brussels. Data protection authorities, MEPs, European airlines, and invited academics and experts all stressed their concern that human rights and data protection are being bypassed by the European Commission and Council.

The main conclusions stated that any future PNR deal with the US must respect fundamental rights and provide adequate safeguards. The issues addressed focused in particular on how personal data should be transferred to US law enforcement agencies in the future. Despite the fact that the Interim Agreement foresaw to change from “pull” to “push” system, the participants stressed that there were no technical obstacles impeding “push” system and that the contracting parties were called upon to find ways to remedy the present situation.

Peter Schaar, chairman of the Article 29 Working Party, stated at the seminar: “Any new agreement must of course meet legal requirements, but we also have to look at possible technical safeguards, such as anonymising or pseudonominising the data. Wouldn't it be sufficient if the identity of a passenger were revealed to the US authorities only once their screening systems have found indications for a suspect? There must be proof that practices meet the requirements, including the requirement that they are necessary, not just useful for the US side. The way to ensure this is an

independent audit of the practices, to be carried out jointly by both sides and including data protection authorities."[50]

Other seminar's criticized points included:

- unclear purposes for which the data is used;
- uncertainty regarding how PNR data is actually being used;
- lack of data protection in the US;
- no protection at all for non-US citizens by the US Privacy Act;
- flaws in programs such as Secure Flight and the ATS, which exceed the terms of the PNR agreement;
- parallel activities that bypass the current interim PNR agreement (for instance, the Open Skies treaty[51]);
- the number of fields in the PNR and their content;
- lack of independent review of the current PNR agreement;
- lack of clear justification for US government access to PNR, or evidence of its effectiveness;
- usage of a program justified as an anti-terrorist measure primarily for general law enforcement and border control.

Recommendations from the experts included that the LIBE Committee, EP, and the Article 29 Working Party should:

- Insist on inclusion of representatives of national data protection and human rights authorities and experts in national delegations to ICAO plenary meetings and ICAO task forces and working groups.

---

[50] EurActiv.com, *Privacy experts take on Commission over US data deal*, 27 March 2007. http://www.euractiv.com/en/infosociety/privacy-experts-take-commission-us-data-deal/article-162785

[51] The Open Skies Treaty of 1.01.2002 currently has 34 States Parties. It establishes a program of unarmed aerial surveillance flights over the entire territory of its participants. http://www.state.gov/www/global/arms/treaties/openski1.html

- Insist on inclusion of national data protection and human rights authorities and the LIBE Committee in the current European Commission consultation on the Code of Conduct for CRS's. Insist that the current consent and notice requirements for disclosure of CRS usage and of data transfers to commercial or governmental third parties be retained, and that the EC begin to enforce them.
- Insist that the Open Skies agreement explicitly recognize the right to freedom of movement guaranteed by Article 12 of the International Covenant on Civil and Political Rights and other instruments of international law, and that the Open Skies agreement not preempt the PNR agreement or require compliance with national "security" measures not subject to meaningful independent judicial review to assure their compatibility with principles of human rights and civil liberties.
- Enforce the requirements of the Directive and national data protection laws with respect to transfers of PNR data to the US, in light of the lack of adequate protection for PNR data in commercial hands, once it is transferred to the US. This enforcement effort should begin from a recognition of the reliance of airlines, travel agencies, tour operators, and other travel companies on CRS's as aggregators and processors of travel data, and should therefore focus on the obtaining compliance by the CRS's.
- Ensure that the use of any PNR or APIS data collected from travellers or other data subjects in response to government mandates is limited to government purposes. Airlines, CRS's, and other travel companies should not be given a "free pass" to retain, use, disclose, or transfer this data commercially after it has been obtained by government coercion[52].

As the negotiations of the PNR issue between US and EU continued, during his visit to Brussels on 14 May 2007, US Homeland Security Secretary Michael Chertoff asked for more relaxed restrictions on the personal data transfer from the airline companies. One of the restrictions Chertoff referred to in asking for looser conditions

[52] Written Testimony of Edward Hasbrouck before the LIBE Committee of the European Parliament and the Article 29 Working Party. Brussels, 26 March 2007.

was the use of the data limiting their dissemination to institutions that have strict privacy safeguards standards as in the EU. Chertoff considered that in order to stop terrorism, the data had to be shared among all US government agencies. He also stated the US wanted to hold the data for 40 years but he also said this was negotiable. Chertoff claimed that "PNR data is protected under the US Privacy Act and the Freedom of Information Act, among other laws, as well as the robust oversight provided through [...] American courts."[53]

However, it was obvious that the Privacy Act applied only to US persons, not EU citizens and residents: pursuant to Privacy Act section (g)(1), in certain cases "the individual may bring a civil action against the agency". But according to section (a)(2), "the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence"[54].

2.2.5 PNR Agreement 2007

On 23 July 2007 the Council adopted a decision authorising signature of a new agreement on the PNR issue[55]. The agreement was signed on 23 July 2007 on behalf of the EU and on 26 July 2007 on behalf of the US (PNR Agreement 2007). It states that "for the application of this Agreement, DHS is deemed to ensure an adequate level of protection for PNR data transferred from the European Union" (Paragraph 6).

---

[53] Michael Chertoff, letter to Members of EP, 14 May 2007.
http://useu.usmission.gov/Dossiers/Data_Privacy/May1407_Chertoff_EP_Letter.pdf
[54] Text of the Privacy Act 5 USC Sec. 552a (01/16/96).
http://usgovinfo.about.com/library/foia/blprivacyact.htm
[55] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record data by air carriers to the United States Department of Homeland Security.

But the problem that this Agreement, just like the previous deals, has actually no legal force or effect for the US remains. It has been neither enacted into US law nor ratified by the US Senate as a treaty.

With reference to the EU Member States, the Agreement is binding for them, but before it is ratified and incorporated, the PNR transfer can be governed only by national law and is generally prohibited (this issue has been discussed in 2.2.1). On 23 July 2007 11 Member States indicated that, in order for the Council to conclude the Agreement, they would have to comply with the requirements of their constitutional procedures. According to the information of the EU Council, by 19 March 2009 only five of the EU Member States have finalized the ratification/incorporation process.[56]

The new arrangement consists of the following elements:

(i) the Agreement signed by both parties;

(ii) US letter to EU (DHS letter) giving assurances on the way it intends to protect PNR data; and

(iii) EU letter to US, which is a reply letter from the EU acknowledging receipt of the assurances and confirming that on the basis of the assurances it considers the level of protection of PNR data in the US as adequate.

Notwithstanding the validity of the Agreement for the US mentioned above, formally the Agreement is a treaty. But what is the legal status of the letters?

Vienna Convention on the Law of Treaties 1969 provides for a document to be considered a treaty "whatever its particular designation" (Article 2). According to

[56] Council Decision 5311/1/09 of 19 March 2009 on Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) - Declarations made in accordance with Article 24 (5) TEU – State of Play.

Article 11, the consent of a State to be bound by a treaty may be expressed, inter alia, by exchange of instruments constituting a treaty.

Furthermore, Article 13 stipulates that "The consent of States to be bound by a treaty constituted by instruments exchanged between them is expressed by that exchange when: (*a*) the instruments provide that their exchange shall have that effect; or (*b*) it is otherwise established that those States were agreed that the exchange of instruments should have that effect".

In practice, if the instruments exchange is not meant to be binding, the words "understanding" and "arrangements" are used instead. In our case, we can find neither the classic phrases to indicate that the letters constitute a treaty, nor the classic phrases to indicate that they do not. Thus, to determine whether the letters are intended to be binding, the text of the Agreement should be analyzed.

The Agreement gives reference to the DHS letter in Paragraph 1, but does not state that the US shall implement the safeguards in the letter. It only states that the US shall process PNR data in accordance with domestic law (Paragraph 3). The agreement can be denounced by the EU if the EU determines that the US has breached it (Paragraph 3); there is no explicit reference to the US breaching the safeguards in the DHS letter.

"It seems clear that the parties wished to leave the legal effect of the letter ambiguous, or that they could not agree on the precise legal status of the letter. The best view, although the issue is far from doubt, is that the parties have agreed that the letter, while not binding in itself, is closely connected to the operation of the treaty, as it is an express condition of entering into the agreement (on the EU side) and will be revoked in the event of a breach of the agreement by the EU (on the US side). It also appears implicitly that if the safeguards in the letter are not applied in practice, in the

view of the EU, then the EU will consider that this is valid grounds to denounce the treaty" [57].

Therefore we cannot state that the letters are legally binding. It is more accurate to say that they have an indirect legal force, since the EU has entered into the treaty on the basis of the assurances in the DHS letter explaining its safeguarding of PNR.

The key points of the deal are as follows.

DHS letter Paragraph I provides that "DHS uses EU PNR strictly for the purpose of preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above. PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law". As we can see from this text, the list of purposes is not limited at all.

DHS can share PNR data with "other domestic government authorities with law enforcement, public security, or counterterrorism functions, in support of counterterrorism, transnational crime and public security related cases (including threats, flights, individuals and routes of concern) they are examining or investigating, according to law, and pursuant to written understandings and US law on the exchange of information between US government authorities" (DHS letter Paragraph II). Again, the list of authorities is not limited.

The dataset was reduced from 34 to 19 elements (the full list is available in Annex 3 hereto). But the reduction is largely cosmetic due to the merging of data fields instead

[57] Steve Peers, *The legal status of the Agreement and letters*, Statewatch, 3 July 2007. http://www.statewatch.org/news/2007/jul/03eu-pnr.htm

of actual deletion. See, for example, DHS letter Paragraph II, line 7: ”All available contact information (including originator information)”. Previously (Undertakings 2004, Attachment ”A”) they constituted 4 separate data items:

- 6. Address,
- 9. Contact telephone numbers,
- 17. E-mail address,
- 28. Received from information.

The same concerns lines 8, 10, 14, 16 and 17.

With regards to sensitive data, it is stated that “DHS employs an automated system which filters those sensitive PNR codes and terms and does not use this information” (DHS letter Paragraph III). But the same paragraph provides that the sensitive data can be accessed for an exceptional case: “If necessary, in an exceptional case where the life of a data subject or of others could be imperiled or seriously impaired”.

It was claimed that for the first time that EU citizens would also be covered by the US Privacy Act which meant they could enforce their rights in US courts (DHS letter Paragraph IV)[58].

The US is allowed to store the data in an active analytical database for seven years, after which time the data will be moved to dormant, non-operational status and can be accessible under stricter rules. This means a 15 year storage period in total as compared to three years as previously agreed (DHS letter Paragraph VII).

PNR Agreement 2007 received harsh criticism from the EP, Article 29 Working Party, EDPS, as well as on the national level.

[58] However, on 22.08.2007 the US announced changes in the Privacy Act that gave exemptions from responding to requests for personal information held to DHS and ATS (see 2.3.1).

In a letter dated 27 June 2007 to the German interior minister Wolfgang Schauble, EDPS Peter Hustinx showed concern arguing that the privacy rights of air passengers between the EU and US will be threatened by the new agreement. On 12 July 2007 the EP adopted a Resolution[59] that heavily criticized the new PNR agreement, considering it "substantively flawed", in particular by "open and vague definitions and multiple possibilities for exception". EP stated that the agreement "had been concluded without any involvement of the EP, lacking democratic oversight of any kind". Article 29 Data Protection Working Party issued an opinion on the new PNR agreement, which concluded that "in general, the safeguards provided for under the previous agreement have been markedly weakened", and "the new agreement leaves open serious questions and shortcomings, and contains too many emergency exceptions".[60] The Working Party, as an official EU data protection advisory body, had not been consulted or asked for advice on the data protection elements of the agreement. Moreover, the Directive on API[61] and the EU's PNR agreements with Australia[62] and Canada[63], which ensure higher standards of protection of personal data, have not been taken into account while negotiating the Agreement.

In summary, the weak points of the Agreement are:

---

[59] European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America.

[60] Article 29 Working Party, Opinion 5/2007 of 17.08.2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007.

[61] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

[62] Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service. 8.8.2008. Official Journal of the European Union (L 213/51).

[63] Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data. 21.3.2006. Official Journal of the European Union (L 82/15).

- Lack of legal certainty: the handling, collection, use and storage of personal data from air passengers by DHS is not founded on a legal agreement but on non-binding assurances remitted in a letter.
- The new agreement states that it applies to airlines operating to and from the US. It is not clear whether this includes, for example, airlines operating from a third country who transit through the EU. It is not clear where the limits are of EU jurisdiction. Is it the processing operation or the data controller who is based in the EU?
- Lack of purpose-limitation: PNR transfer is not limited to fighting terrorism; it can also be used for other "unspecified additional purposes" by the US government.
- Despite the willingness of the DHS to move to the "push" system no later than 1 January 2008 in principle, the shift – already foreseen in the 2004 PNR agreement – has been delayed for years, even though the condition of technical feasibility has long since been met. The "push" system for all carriers should be a *sine qua non* for PNR transfers. But it remains unclear if and under what conditions this new method of transfer will eventually be worked out. It also remains unclear how DHS, allowed in exceptional cases to retrieve data other than those listed, may access such data after the transition from a "pull" to a "push" system.
- Joint periodical review by DHS and EU does not provide any involvement of EDPS or national data protection supervisors, which was provided for under the previous PNR agreement. It remains unclear when and under what circumstances a joint review will take place. The agreement does not foresee any mechanism aimed at resolving disputes, leaving it up to the contracting parties. This is particularly relevant for a joint review.
- Since passengers must be properly informed of the use of their data and their rights, and that this obligation rests with the airlines, DHS and the Commission must take responsibility for the information provided to passengers and the "Short notice for travel between EU and US" must be made available to all passengers.

- Despite the fact that the US Privacy Act will be extended administratively to EU citizens, DHS reserves the right to introduce exemptions under the Freedom of Information Act. EU citizens' PNR data are to be treated solely according to US law, without an adequacy assessment or any indication of the specific US legislation applicable. Thus the absence of a robust legal mechanism that enables EU citizens to challenge misuse of their personal information.
- Extension of the time the data are kept, introducing a concept of “dormant” data. Data can be retained for longer periods with the new agreement - from 3,5 years to 15 and the period might be even longer. There is no guarantee that the data will be definitively deleted after the 15 year period. Besides that, PNR data will be kept for seven years in “active analytical databases”, leading to a big risk of massive profiling and data mining, contrary to EU principles.
- The reduction of PNR data fields from 34 to 19 is cosmetic. Moreover, the elements include information on third parties other than the data subject.
- Sensitive data will be made available and can be used by DHS in exceptional cases, which was excluded by the previous agreement. In addition, the filtering of sensitive data continues to be done by DHS even with a “push” system.
- Apart from “exceptional cases”, sensitive data can be contained within the mandatory 19 fields of data. DHS letter Paragraph II, Line 17 (“OSI, SSI and SSR information”) can include such items as special meal requests, which can give an idea about religious beliefs of the passenger and thus constitute sensitive data.
- The agreement fails to define precisely which US authorities may access the data.
- There is no limitation to what US authorities are allowed to do with the data.
- The data regime of onward transfers by third agencies to other units is unclear.
- The envisaged transfer of analytical information flowing from PNR data from the US authorities to police and judicial authorities in the Member States, and

possibly to Europol[64] and Eurojust[65], outside the framework of specific judicial procedures or police investigations, as mentioned in the DHS letter. This should only be allowed in accordance with the existing EU-US agreements on mutual legal assistance and extradition.

- Third countries may be given access to PNR data if adhering to DHS-specified conditions, and that third countries may exceptionally, in unspecified emergency cases, be given access to PNR data without assurances that the data will be handled according to the DHS level of data protection. Moreover, EU has accepted 'not to interfere' with regard to the protection of EU citizens' PNR data that may be shared by the US with third countries.
- The agreement runs the risk that that any change in US legislation might unilaterally affect the level of data protection as foreseen in the PNR agreement[66].
- It is unclear what the effects of the provisions on reciprocity mean for the level of data protection in any EU PNR regime. Art. 5 of the new agreement and Article IX of the DHS letter (on reciprocity) contain an ambiguous statement about the US side's expectations of the data protection measures applied to both the US and any future EU PNR regime. While it is expected that this means that the US does not expect lower standards in a future EU PNR regime than the ones in the new agreement, it could also be interpreted as meaning that the DHS is asking the EU not to put in place higher data protection standards in an EU PNR regime, or they will suspend the agreement.
- The Agreement regulates PNR, but not API. Initially, API contained few data types and were used solely for air transportation purposes. Their transfer could thus rest on Article 26(1)(b) of the Directive (performance of the transportation contract

[64] Europol is the European Law Enforcement Organisation which aims at improving the effectiveness and co-operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of international organised crime. http://www.europol.europa.eu/

[65] Eurojust is a EU body established in 2002 to enhance the effectiveness of the competent authorities within Member States when they are dealing with the investigation and prosecution of serious cross-border and organised crime. http://www.eurojust.europa.eu/

[66] See section 2.3.1.

between data subjects and carriers). However, since 2001 the amount of API increased and their processing purpose was extended to include public security. The content of API became similar to PNR. The former allow the tracing of the routes of European passengers in a manner just as precise as the latter; nevertheless, no privacy protection guarantees are given in respect to API[67].

Therefore new deal still failed to offer an adequate level of data protection and left many problems open.

[67] See: Ioannis Ntouvas, *supra* n 11.

2.3 After Agreement Phase

2.3.1 Further Requests from the US

Just seven days after the PNR Agreement 2007 was signed, the US government wrote to the EU Council asking it to agree that the negotiations and all the negotiating documents (including e-mails) leading to the agreement be kept secret for at least ten years after the entry into force of the agreement[68].

The EU reply said that "the European Union shares your understanding regarding the confidentiality of the negotiation process"[69]. Moreover, it added that "Article 4, paragraph 1(a), third indent of the Regulation 1049/2001 obliges the institutions to refuse public access to a document where disclosure would undermine the protection of the public interest as regards international relations", while any request for access to a document "must be examined and replied to on a case-by-case basis. Obviously, such a request will always be evaluated in good faith, keeping in mind the US expectations regarding confidentiality of negotiation documents, as expressed in your letter of 30 July 2007, and with due regard for the applicable EU legislation." In other words, people can apply for these documents and the request will be examined "with due regard for the applicable EU legislation" in the context of "US expectations".

Article 4.4 of the Regulation deals expressly with access to documents from third parties (i.e. non-EU states like the US). This says that the institution (the Council) shall "consult the third party with a view to assessing whether an exception in

[68] The letter from Paul Rosenzweig, Acting Assistant Secretary for Policy at the DHS, to the EU Council Presidency, 30 July 2007. EU doc no: 12307/07.
[69] Council Decision 12309/07 of 31 August 2007 on Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) - Letter on confidentiality of negotiation documents.

paragraph 1 or 2 is applicable, unless it is clear that the document shall or shall not be disclosed".

How the EU intends to effect this commitment to refuse access on the grounds of "the public interest as regard international relations" is not clear. Already the Council's own public register of documents gives access many full-texts of documents falling under this so-called confidentiality rule. Are these documents going to be removed?[70]

Furthermore, on 22 August 2007 the US government announced some changes in its Privacy Act that gave exemptions from responding to request for personal information held to DHS and ATS[71].

The exemptions related to the new Arrival and Departure System (ADIS) that the US was to introduce. ADIS is intended to authorise people to travel only after PNR and API data has been checked and cleared by the US watch lists. "DHS is republishing the Privacy Act system of records notice for ADIS in order to expand its authority and capability to serve additional programs that require information on individuals throughout the immigrant and non-immigrant pre-entry, entry, status management, and exit processes."[72]

There were also changes to the rules under the US Privacy Act to exempt ATS[73]. Although created to combat terrorism, the ATS covers "other crimes" and any activity in violation of the US law. ATS maintains PNR and the use of PNR data is explicit.

---

[70] Statewatch, *US demands 10 year ban on access to PNR documents*, 2.09.2007. http://www.statewatch.org/news/2007/sep/02eu-usa-pnr-secret.htm.
[71] Privacy Act of 1974: Implementation of Exemptions; Redress and Response Records System. Federal Register: 18 January 2007 (Volume 72, Number 11).
[72] Proposed Rules, Federal Register - DHS, 6 CFR Part 5, Privacy Act of 1974: Implementation of Exemptions, 22.08.2007.
[73] See *supra* n 71.

The exemptions seem to be meant to counterbalance "the set backs" for the US government in the 2007 PNR Agreement. When the agreement was signed the Council and the Commission relied upon the extension of protections in the US Privacy Act to travellers from the EU (see). In DHS letter Paragraph IV it is stated that DHS has taken the decision "to extend administrative Privacy Act protections to PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens. Consistent with US law, DHS also maintains a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information about or correction of PNR." The introduced exemptions contradict this statement.

"The adoption of these two exemptions will seriously diminish any rights EU citizens have to find out what data is held on them and who it is held by. Did the Council and the Commission, who negotiated the agreement, know the US was planning to introduce them, and if not why not? […] Yet again we see the US telling the EU what to do. […] US access to PNR data and its further processing is an issue of substantial public interest which directly effects the rights and privacy of EU citizens and therefore all the documentation should be in the public domain for parliaments and people to see and discuss. It is a quite outrageous request and it is even more outrageous that the EU is going to agree to it," stated Tony Bunyan, Statewatch editor [74].

2.3.2 Move Away from Single Approach

Just after six months after signing PNR Agreement 2007, the US attempted to force countries like Greece, the Czech Republic and Estonia to transfer additional

[74] Statewatch, *US gains new advantages in the EU-USA PNR agreement*, 12 September 2007. http://www.statewatch.org/news/2007/sep/12

information on transatlantic passengers and allow armed air marshals on board in exchange for visa-free travel to America.

Currently, the US Government refuses to grant visa-free access to the EU as a whole. Citizens from 15 of the EU 27 Member States can travel for short stays without a visa to the US under the Visa Waiver Program (VWP). It is a long-stated goal of the EU that all Member States be treated equally and received visa-free access.

In August 2007 the US adopted new legislation which provided for the modernization of the VWP. The US proposed a draft Memorandum of Understanding (MoU) to EU Member States individually covering the security provisions of this new legislation. But several conditions for the implementation of the VWP reform fall under the responsibility of the European Community to negotiate on the Member States' behalf.

“We don't negotiate matters that are dealt with in Washington with the state of California. That would be disrespectful and we expect the United States to be similarly respectful of our law and system,”[75] said the Commission's Director General for Justice and Security Jonathan Faull on 13 February 2008.

Czech and Estonian governments confirmed they had talks with US officials, but they insisted they were taking EU law into account. However, within one year after the signing of PNR Agreement 2007, a small group of EU Member States signed up to their own MoU with the US in respect of visa waivers which could potentially jeopardise the protection afforded to passenger data collected in those countries and extend beyond the remit of data required to be provided under the PNR Agreement 2007.

---

[75] Charlemagne, *America plays divide and rule*, Economist.com, 14 February 2008. http://www.economist.com/blogs/certainideasofeurope/2008/02/america_plays_divide_and_rule.cfm

The Czech Republic's MoU with the US signed on 26 February 2008 provoked widespread concern. “In this MoU Czech authorities agreed to ‘passenger and other information sharing, screening information concerning known or suspected terrorists, information to combat terrorism and serious crime, and information on migration matters’ with the US authorities and also promised to ‘allow for the further dissemination of transferred information within the US Government’. Czech Ministry of Interior agreed ‘to provide identifying information that includes biographic and biometric data, to be used in determining whether persons who intend to travel to the United States represent a threat to the security, law enforcement, and immigration interests of the United States’. […] In the new MoU, the Czech Ministry of Interior declares its intention ‘to collect, analyze, use, and share API’ and ‘to collect, analyze, use, and share PNR’.”[76]

Following the Czech Republic‘s MoU, similar bilateral documents were signed by other five new EU member countries: Estonia, Latvia, Lithuania, Hungary and Slovakia.

The EU had to undertake some actions. On 18 April 2008 the European Council authorised the European Commission, on behalf of the European Community, to open negotiations with the US on certain conditions for access to the VWP. Such negotiations were supposed to be open to ensure that both tracks, the Community one and the national one, proceed in parallel, with the ultimate aim of all Member States taking part in VWP.

The individual negotiation by Member States who are currently not members of VWP is weakening the united position of Member States as a whole, and it is a concern that

[76] European Digital Rights, *Czechs became Trojan horses for new US visa waiver programme*, 26 March 2008. http://www.edri.org/edrigram/number6.6/czech-us-visa-waiver

differing concessions are being made in MoU signed between Member States and the US. The US' constant push for more personal data from the EU citizens continues.

2.3.3 DHS Report 2008 and Real Life

On 19 December 2008 DHS released a report concerning PNR information derived from flights between the US and the EU[77].

The authors of the report conclude that DHS handling of PNR data "is in compliance with both US law and the DHS-EU agreement on USA access to, and use of, PNR data related to flights between the EU and the USA."

However, according to the PNR Agreement 2007, there should be periodic joint US-EU reviews of compliance, while the report was just a unilateral internal review conducted within the DHS, which did not include any EU representatives.

The US human rights association Identity Project (IDP) published a condemnation on its website of a series of violations of the PNR Agreement 2007[78], in particular the enormous difficulties encountered by citizens wishing to exercise their right to access stored data concerning them (which are frequently sensitive, such as health data and meal preferences, *etc*.).

IDP stated the following:

---

[77] A report concerning Passenger Name Record Information derived from flights between the US and the European Union (18.12.2008).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.

[78] See: http://www.papersplease.org/wp/2008/12/24/dhs-admits-problems-in-disclosing-travel-surveillance-records/#more-262

> The DHS had legal obligations to US citizens and residents under the Privacy Act, and commitments to travellers from the EU under PNR Agreement 2007, to allow individuals timely access to PNR data about them held by the DHS. According to the report:
> "DHS policy allows persons (including foreign nationals) to access and seek redress under the Privacy Act to raw PNR data maintained in ATS".
> Despite this, the DHS Privacy Office has now reported that:
> 1. Requests for PNR data have typically taken more than a year to answer — many times longer than the legal time limits in the Privacy Act and Freedom of Information Act: "The requests for PNR took more than one year to process."
> 2. When individuals have requested "all data" about them held by the DHS, often they have not been given any of their PNR data: "If an individual requests 'all information held by CBP' the FOIA specialist generally does not search ATS because PNR was not specifically requested."
> 3. Because of this, the vast majority of requesters who should have received PNR data did not: "The PNR specific requests are a small percentage of the total requests based on the statistics provided to the Privacy Office, but if ATS were searched in all cases in which an individual asks for 'all information held by CBP,' the percentage would increase"
> 4. PNR data has been inconsistently censored before it was released: "The requests for PNR […] were inconsistent in what information was redacted."
> 5. A large backlog from the initial requests for PNR data remains unanswered, more than a year later: "Management noted that they have been understaffed and are bringing on new staff to reduce the backlog and period of time it takes to respond to requests. Additionally, management stated that part of the delayed response was due to the large number of requests initially submitted for PNR."

An example of such violations was the request in 2007 from MEP Sophia In 't Veld to get her PNR information. At first she received a claim from DHS that they did not have any record of her trip. The MEP finally received her PNR data after American lawyers filed a Federal lawsuit[79] on her behalf, but the data was "late, clearly incomplete, and inconsistently and inappropriately redacted"[80].

[79] The full complaint: http://www.eff.org/files/int_veld_complaint.pdf.
[80] Edward Hasbrouck. *Can you really see what records are kept about your travel?* 30.12.2008. http://hasbrouck.org/blog/archives/001595.html.

Therefore, the report actually showed a number of weaknesses proving that the DHS has complied with neither the PNR Agreement 2007, nor the US law (especially, but not only, the Privacy Act) in its use of PNR data concerning US citizens as well as Europeans.

CBP/DHS, when accessing PNR and secretly keeping copies of some of them in ATS, violated the Privacy Act which requires prior notice in the Federal Register, in specific form, of the existence, content, and usage of each system of records of personal information maintained by a US Federal agency. Only in 2006, after years of illegal operation outside the Privacy Act and EU laws and regulations, the CBP/DHS confirmed the existence of the ATS and US government retention of PNR data[81].

But what about the opportunity of getting records from the other side of the Atlantic? Under the Directive, the travellers have the right to see all of the records concerning them kept by companies, and to be told what data has been sent to other parties.

But when one of American privacy advocates, Edward Hasbrouck, asked KLM Royal Dutch Airlines to see the records of one of his trips from the US to the EU and back, and to be told what third parties had accessed his records, they told him that no one had ever asked any European airline for those details before. KLM had no procedures for complying with the law regarding such case. After months KLM informed that:

(i) they had outsourced the handling of his data to companies in the US;

(ii) they did not know what data their contractors and agents had collected or retained, or with whom they might have shared the data; and

(iii) they had no provisions in their contracts that would enable them to force their contractors to provide this information[82].

---

[81] http://www.papersplease.org/wp/2008/12/24/dhs-admits-problems-in-disclosing-travel-surveillance-records/

[82] See Edward Hasbrouck, *supra* n 80.

When Edward Hasbrouck asked the Dutch Data Protection Authority to intervene, it was the first formal request that they had received regarding airline reservations. They also admitted that they had no staff with the technical competence or industry knowledge to interpret the limited data that KLM had disclosed, or to assess the validity of KLM's claims. A year after the original request to KLM for travel records, the Dutch authorities informed they could not help, and that Edward Hasbrouck could do nothing more unless, within 45 days, hiring a lawyer in the Netherlands to prepare and file a private lawsuit, at his own expense, in Dutch, in a Dutch court, against the airline.

Therefore, these real-world experiences prove that neither American nor Europeans can rely on DHS, airlines and travel companies' compliance with the existing rules. Legal rights and promises with respect to travel records have proven unenforceable both in the US and the EU, for both US and EU citizens.

2.4 Proposed European PNR System and Other Plans

Just a few days after the car bomb attack in Glasgow and London[83], the Commissioner Franco Frattini announced that he would propose a new draft containing anti-terrorism measures, including creating a European PNR system. In his speech in front of MEPs he stated: "Up until now, PNR has been associated mostly with negotiations aimed at securing that EU citizens data are correctly processed by our partners and allies, in particular the United States. The Commission thinks the time has come to change focus and devote resources to the security of the Union. The Union is at least as much a potential target of a terrorist attack as the United States and the use and analysis of Passenger Name Records is an important law enforcement tool, to protect our citizens."[84].

In November 2007, the EU announced the project[85]. The plan was similar to the PNR Agreement 2007. According to the proposal, airlines make available to the Member States 19 PNR data elements of their passengers. Such data must be made available only for flights to and from the EU (excluding intra-EU or domestic flights). EU carriers will be required to "push" the data to the Member States authorities. There will be two data transmissions, one 48 hours before the flight take off and one when the flight is all boarded. The recipient of the data in the Member States will be a Passenger Information Unit (PIU) to be designated in each Member State. PIU will make a "risk assessment" of the traveler, which could lead to the questioning or even refusal of the entry. PIU will share the results of such assessments with other PIU where necessary and retain the data for 5 years in an active database and for 8 years

[83] On 29 June 2007, in London, two car bombs were discovered and disabled before they could be detonated. The Glasgow International Airport attack occurred on 30 June 2007.
[84] Franco Frattini. *EU counter-terrorism strategy*. European Parliament, Strasbourg, 5 September 2007. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/07/505.
[85] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, Brussels, 28 November 2007.

in a dormant database. Airlines refusing to provide the requested data before take-off will be threatened with the withdrawal of their landing authorisation.

Some Member States already adopted such measures at the national level. The proposal states that "once the EU framework is adopted and operational, it will provide all Member States and air carriers with a single and coherent legal environment in this field".

On the one hand, the draft makes references to the Framework Decision on Data Protection in criminal matters, which will govern all data processing under the proposal, as well as the transfers of data to third countries, stating that "no sensitive data will be used and there will be no enforcement action taken solely on the basis of the automatic processing of PNR". Also, the draft mentions the Council Directive 2004/82/EC, which provides that air carriers are obliged to communicate API to the competent authorities of the Member States, which are used for fighting illegal immigration. According to the Proposal's text, "The added value of PNR is that it helps identify unknown people and develop risk indicators". On the other hand, the draft makes no reference to the Data Protection Directive.

The plan was criticized by the EP, the Article 29 Working Party and the EDPS, as well as by legal experts and human rights groups, who opposed the plan and found it a threat to privacy.

In its Resolution of 12 July 2007 on the PNR agreement with the US, the EP stated that, since any PNR data in such a system may be made available to the DHS, the Commission must "clarify the state of play with regard to an EU PNR system, including making available the feasibility study it has pledged to undertake" (Paragraph 27). In Paragraph 28 the EP asked the Commission to substantiate:

a) the operational need and purpose of collecting PNR data at the point of entry into EU territory;
b) the added value of collecting PNR data in the light of the already existing control measures at the point of entry into the EU for security purposes, such as the Schengen system, the Visa Information System, and the API system;
c) the use that is envisaged for PNR data, in particular whether it is for identifying individuals in order to ensure air security, for identifying who enters the territory of the EU, or for general negative or positive profiling of passengers.

Article 29 Working Party expressed serious concerns in its press release dated 6 December 2007[86]. In its view, "The proposal is too closely modelled on the recently signed EU-US PNR agreement to be a balanced legal instrument".

In particular, the Working Party highlights the following shortcomings:

- the proposal does not substantiate any legitimate basis for the collection of passenger data;
- the amount of personal data collected is unreasonable;
- the retention period of 13 years seems to be excessive;
- inadequate filtering mechanisms and possible third-country transfers.

The EDPS issued an opinion[87] critical of the following elements:

- insufficient justification of the legitimacy of the measures in view of the purpose of combating terrorism;
- serious lack of legal certainty;
- lack of clarity about the identification of the data recipients;
- potential data transfers to third countries.

---

[86] Available at: http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_05_12_07_en.pdf
[87] Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement Purposes (2008/C 110/01).

The European airlines criticized the proposal as well: “Despite assurances from the Commission that the proposal would not put any extra burden on airlines, because they already have all the information and are already required to communicate passport data to member states' competent authorities in order to fight illegal immigration, the AEA said the proposal fails to take account of the practical consequences for both European carriers and their passengers”[88].

According to AEA, “Commissioner Frattini's proposed decentralised system means that our carriers will have to comply with 27 different national data collection systems. We are talking about an operational and technical nightmare – and the Commission totally ignores the financial implications for the airline industry, which we haven't even started assessing yet.”[89]

Nevertheless, some European member states, with the UK in the lead, wanted to go much further, proposing the following:

- the European PNR system should cover not just flights in and out of the EU but also flights between EU countries plus all flights within each country;
- the system should cover not just all flights but all sea and land travel as well;
- the data and information gathered should be used not just for entry-exit but also for any law enforcement purpose[90].

---

[88] EurActiv.com. *Association of European Airlines (AEA): European airline body dismayed at proposal for EU-PNR system*, 9 November 2007. http://www.euractiv.com/en/transport/passenger-screening-plan-nightmare-airlines/article-168216.

[89] Association of European Airlines. *European airline body dismayed at proposal for EU-PNR system*, 08 November 2007. http://www.aea.be/assets/documents/press/Pr07-029.pdf

[90] Statewatch, *Observatory: EU surveillance of passengers (PNR)*. http://www.statewatch.org/eu-pnrobservatory.htm

As a result, in October 2008 the European Council started re-writing the proposal for an EU PNR scheme[91]. The key features of the EU PNR regime are still under negotiations and consideration.

According to the draft text proposed on 17 April 2009, "This Framework Decision provides for the transfer or the making available by air carriers of PNR data of passengers of international flights to the Member States, for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious crime, as well as the processing of those data, including their collection, use and retention by the Member States and their exchange between them".

Other important issues include:

- The EU-PNR scheme would cover air traffic between the EU and third states, including transit passengers.
- The retention period is three years (Article 9); it is indicated in a footnote that "no consensus has been reached yet on the question of the exact length of the additional retention period".
- PNR data and the analysis of PNR data may be transferred or made available by a Member State to a third country.
- Since 27 EU countries have watch lists which are extremely different, the proposal suggests the necessity of developing 'common methods and indicators'.
- The choice of individual states to take the measure at the national level should be explicitly recognised. This means that actually the PNR will be collected by all Member States on all flights in and out of the EU and if a Member State wants to survey intra-community flights as well, it can very well do it.

[91] See Council Decisions on Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes: 13803/1/08 of 9 October 2008; 14592/08 of 21 October 2008; 16457/08 of 28 November 2008; and 5618/1/09 of 17 April 2009.

In August 2008, the "Future Group" of Interior and Justice Ministers from six EU member states (Germany, France, Sweden, Portugal, Slovenia, and the Czech Republic) drafted a report suggesting a series of proposals "to boost EU integration in policing and intelligence-gathering, including the creation an EU-US Area of cooperation for 'freedom, security and justice'"[92]:

- EU Member States should pool information in a central intelligence unit, creating a network of "anti-terrorist centers", standardising police surveillance techniques and extending the sharing of DNA and fingerprint databases to include CCTV video footage and material gathered by "spy drones".
- The European Gendarmerie Force should be expanded into an EU body that could be used for paramilitary intervention overseas.
- Euro-Atlantic pact of cooperation with the US should be concluded. The document needs to be finalized by 2014 at the latest and would not just cover terrorism and passenger data but would cover the whole area of justice and home affairs – policing, immigration, sharing database data and biometrics.

With regards to the pact, there can appear a problem due to the difference in privacy regulation between EU and US, but the US seems to push hard for this new pact. Bruno Waterfield, a correspondent for The Daily Telegraph has expressed the way in which security has been escalated to a level that he calls 'securocracy': "This concept heralds a new era by standardising European police surveillance techniques and creating 'tool-pools' of common data gathering systems to be operated at the EU level."[93]

---

[92] Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy („The Future Group"), June 2008, available at:
http://www.telegraph.co.uk/telegraph/multimedia/archive/00786/Read_the_full_EU_re_786870a.pdf

[93] Waterfield, Bruno, *EU plan: The rise and rise of the securocrats*, The Daily Telegraph, 7 August 2008.
http://blogs.telegraph.co.uk/news/brunowaterfield/4841723/EU_plan_The_rise_and_rise_of_the_securocrats/

The European Commission also proposed other new measures:

- Creation of an entry/exit register of non-European visitors to the EU that will record the dates of entry and exit of each non-EU individual admitted to the Schengen visa-free area using biometric identifiers.
- Introduction of a European Border Surveillance System that will use satellites and unmanned aircraft to check on the non-UE travellers on a short-stay visa and to track the movements of suspected illegal migrants. The system is already under construction and may be operational by 2012.

Privacy advocates and MEPs criticized the proposals considering the EU is piling up databases without an overall strategy or a clear vision and believing the EC is only trying to copy the US in their practice to scan fingerprints and pictures of travellers. According to Meryem Marzouki, EDRI board member, "Europe is on its way towards a totalitarian society. As long as there is not adequate data protection under third pillar, there would be no limit to such plans."[94]

The European Commission representatives said that "a legislative proposal will follow", but did not make any statements on when the systems would come into force and refrained from commenting upon criticisms to the lack of EU strategy in dealing with sensitive databases[95].

[94] European Digital Rights, *Biometric data from non-EU travelers*, 13 February 2008. http://www.edri.org/edrigram/number6.3/biometric-eu-travel
[95] See *supra* n 94.

3 Conclusion

As we have discussed, the problems generally derive from the conflict between the US demands for access to information and the EU data protection compliance obligations. There seems to be no sign of either party giving up its position in the immediate future. The fight between EU and US has always been pushy from the side of the US, while EU has always been forced to make steps backwards. EU is trying to fend off US demands; when EU does not cave in the US simply negotiates bilateral deals with individual member states.

The US' point of view can be best illustrated by the following statement of Paul Rosenzweig, Deputy Assistant Secretary for Policy at the US DHS, expressed in November 2007 on the EU "adequacy" requirement: "The EU should reconsider its decision to apply notions of adequacy to the critical area of law enforcement and public safety. Otherwise the EU runs the very real risk of turning itself into a self-imposed island, isolated from the very allies it needs".[96]

The US constantly insists that the scheme for transferring European airline-passenger data to US authorities is insufficient to fight terrorism. Every time the negotiations occur, the US demands more and more the detailed information, enhancing the sharing of data to more and more different US agencies, *etc*.

The protection adequacy is the key issue for the EU, but as far as the US possesses economical measures and flights between the Atlantic apparently must go on, the US

[96] Statewatch, *Observatory on data protection in the EU*, available at: http://www.statewatch.org/eu-dp.htm (detailed history of PNR data conflict).

can afford to be pushy, and we are not in the position to predict any change in this situation, at least in the nearest future. This fact makes the privacy issues dependant on the economic and political needs; thus, the higher standards of the EU privacy law with reference to data transfer to US can hardly be kept. For the time being, the US appears to be winning the battle of access to data. Its constant push for more personal data from EU citizens continues to be ahead of the EU tactical moves to protect its respective position.

In fact, as long as the EU data protection laws exist, those companies that allowed PNR data without the knowledge and consent of data subjects to be sent to the US, have been in ongoing, systematic, routine, and flagrant violation of the EU Data Protection Directive and EU national data protection laws. Moreover, DHS, when accessing PNR and secretly keeping copies of some of them in ATS, violated the US Privacy Act. Since it would have been impossible for DHS to identify which PNR data had been collected in the EU, such access to PNR entailed further violations of EU law by the companies that allowed it without requiring the US government to obtain warrants or court orders for this data.

The report released by the DHS in December 2008 as the result of a unilateral internal review conducted within the DHS, which included neither EU representatives nor any outside experts in PNR data, confirmed lack of compliance with both US and EU laws and showed that the DHS has not fulfilled its commitments to the US or EU travellers.

Real-world experiences undertaken to see if a person can really be informed of his or her records that are being kept and processed, proved that no one can rely on existing compliance, enforcement, or oversight mechanisms both in the US and the EU, for both US and EU citizens.

The practice of PNR transfer was attempted to be legalized by method of concluding bilateral EU-US agreements. An initial agreement of 2004, nonbinding and unenforceable in the US, was ruled invalid by the European Court of Justice, without the court even reaching any of the issues of fundamental rights or adequacy in terms of data protection safeguards. A new agreement, also unenforceable in the US, was signed in 2007.

The weakest points of the Agreement concern:

- its legal force and effect
- inadequate data protection standards
- scope of the agreement uncertainty
- lack of purpose limitation
- “pull”/”push” system issues
- unclear joint review procedure
- extended retention period
- enlarged list of data fields
- sensitive data issues
- API is not regulated
- no clear list of US authorities entitled to access PNR
- problem of enforcement of rights by the EU citizens
- dependence on change in the US legislation, *etc*.

The weaknesses were discovered and discussed broadly in public both before the Agreement had been entered and afterwards as well. There are doubts that those concerns had not been heard by the decision makers. But it must be remembered that they were under strong pressure from the US side and had shortage in time, since the Agreement was needed as soon as possible to avoid legal uncertainties for the EU Member States, air passengers and air carriers. In fact everyone involved in this case, including EU privacy advocates, admitted that it was preferable to have an agreement

with weaknesses and shortcomings, than not to have agreement at all, making it chaos for the air operation across the Atlantic. The Agreement thus was more a political solution than legal instrument. It will undoubtedly need further negotiations and revisions.

Another problem is that the US is still trying to dictate tougher restrictions and get additional data transfer from EU Member States by pushing on them separately. For example, the US takes advantages of the situation that “old” and “new” EU Member States are unequal with regards to American visa policy. But the individual negotiation by Member States with US is weakening the united position of Member States as a whole. The EU is trying to handle with this, but as for now the results cannot be foreseen.

Privacy advocates propose that Europeans should oppose any general agreement on the transfer of personal data from the EU to the US until the DHS has demonstrated that it is complying with the current PNR agreement. In the meantime, persons can exercise their right under EU law to request their PNR and other travel records from these travel companies. Even if the DHS does not tell what information they have obtained, travel companies are required to tell who they have allowed to access the records, and what information they have given to government agencies or other third parties. If they do not, one can complain to national data protection authorities, or bring lawsuit in a European court.

In the case of data processors that are subject to rules that require the provision of data to third parties irrespective of their obligations to the controllers of the data, the first step must always be to make the controller aware of the situation. However, this is easier said than done because any respectable service provider will be wary of doing anything that may highlight a breach of contract to its customer.

A key step that any organisation, either a controller or a processor, should be taking is the assessment of the conflict between the US demands for access to information and the EU data protection compliance obligations in their particular case. From a data protection perspective, a successful controller-processor relationship is one that can deal with this type of situation in an open and collaborative manner. A mutual and ongoing exchange of information about the parties' legal duties should be regarded as one of the most important aspects of their relationship, not just because it will allow those parties to take any necessary pre-emptive action, but because it will be seen by the regulators as a clear sign that these matters are taken seriously.

According to the guidelines laid down by the Article 29 Working Party (Opinion 2/2007), the airlines should provide a simple but efficient data protection guarantee - tell passengers that information about their travel will be transferred to DHS. Of course, informing passengers upon data collection may not in itself legalise the transfer, but would enable them to make a conscious decision, whether they wished to give away their personal details or not.

Another very important issue is as follows. Despite the above-mentioned concerns that the US demands violate the EU law and constitute threat to personal rights in general, in the meantime the EU itself is establishing its own PNR system using the PNR Agreement 2007 scheme as a model, and, moreover, plans to introduce other measures, including new surveillance systems, where such technologies as biometrics will be involved. From these undertakings we can see that the control and surveillance regime designed to struggle for security and prevent terrorism and crimes probably is going to prevail over privacy issues. According to the European Commission's Eurobarometer surveys on data protection of January 2008, the majority of EU citizens (82%)[97] seem to be ready to give up some of their rights and

[97] Eurobarometers are ad hoc thematical telephone interviews to measure public opinion. The survey results are available at: http://ec.europa.eu/public_opinion/flash/fl_225_sum_en.pdf

agree on the monitoring of PNR when this is aimed to combat terrorism (but with the reservation that the monitoring must be restricted to terrorism suspects).

Unfortunately, the scope and purposes of such control can become broader and unlimited. After establishing European surveillance laws, the European Commission might be also seeking to create a global regime on passenger records surveillance, permitting all countries to gain access to this data. Thus, despite the fact that the EU is blaming the US for inadequate data protection standards, it can be going further than the US to establish a global system of surveillance.

References

Judgements

Judgment of the European Court of Justice in Joined Cases C-317/04 and C-318/04, European Parliament v. Council of the European Union and European Parliament v. Commission of the European Communities, 30 May 2006.

Directives / Decisions / Resolutions

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data.

Council Decision 1999/468/EC of 28.6.1999 laying down the procedure for the exercise of implementing powers conferred on the Commission (OJ L 184, 17.7.1999, 23).

Council Decision 12309/07 of 31 August 2007 on Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) - Letter on confidentiality of negotiation documents.

Council Decision 13803/1/08 of 9 October 2008 on Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes.

Council Decision 14592/08 of 21 October 2008 on Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes.

Council Decision 16457/08 of 28 November 2008 on Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes.

Council Decision 5311/1/09 of 19 March 2009 on Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) - Declarations made in accordance with Article 24 (5) TEU – State of Play.

Council Decision 5618/1/09 of 17 April 2009 on Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes.

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 218 of 25 August 2000.

Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, OJ L 235 of 6 July 2004.

European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America.

Treaties / Statutes

Agreement between the European Community and the USA on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security and Bureau of Customs and Border Protection of 28 May 2004.

Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data, 69 Fed. Reg. 41543-41547, 9 July 2004.

Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, 2006 O.J. (L 298) 29.

Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the undertakings issued by DHS on 11 May 2004 in connection with the transfer by air carriers of passenger name record (PNR) data. 27.10.2006. OJ 2006/C 259/01.

Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) of 29 June 2007. O. J. (L 204/18) 4.8.2007

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.01.1981.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23.09.1980.

United Nations Guidelines Concerning Computerized Personal Data Files of 14.12.1990.

European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 1950

Charter of Fundamental Rights of the European Union O. J. C 364/1, 18.12.2000.

Agreement on the European Economic Area of 1 January 1994.

International Covenant on Civil and Political Rights (Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966). 999 UNTS 171.

Vienna Convention on the Law of Treaties, Vienna 23 May 1969

US Privacy Act of 1974, 5 USC Sec. 552a (01/16/96).

Privacy Act of 1974: Implementation of Exemptions; Redress and Response Records System. Federal Register: 18 January 2007 (Volume 72, Number 11).

Privacy Act of 1974: Implementation of Exemptions, Proposed Rules, Federal Register - DHS, 6 CFR Part 5, 22.08.2007.

Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135.

US Intelligence Reform and Terrorism Prevention Act of 17 December 2004.

Opinions

Article 29 Working Party, Opinion 12/98 of 24.07.1998, Transfers of personal data to third countries. Applying Articles 25 and 26 of the EU Data Protection Directive.

Article 29 Working Party, Opinion 2/2004 of 29.01.2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection.

Article 29 Working Party, Opinion 5/2007 of 17.08.2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007.

Article 29 Working Party, Opinion 2/2007 of 15.02.2007 on information to passengers about transfer of PNR data to US authorities.

Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement Purposes (2008/C 110/01).

Letter from European Data Protection Supervisor Peter Hustinx to the German interior minister Wolfgang Schauble of 27 June 2007.

Reports

First Report on “Towards an International Infrastructure for Surveillance of Movement”. Privacy International, in co-operation with European Digital Rights Initiative, the Foundation for Information Policy Research, and Statewatch, with a Commentary from the American Civil Liberties Union on A Perspective from America, February 2004.

DHS, A report concerning Passenger Name Record Information derived from flights between the US and the European Union, 18.12.2008.

Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy of June 2008.

Statements / Comments / Guidelines / Proposals / Memos

Comments of the IATA in respect of: US Immigration and Naturalization Service Notice of Proposed Rulemaking on Manifest Requirements Under Section 231 of the Act 8 CFR Parts 217, 231 and 251 RIN 1115-AG57 (Federal Register/ Vol. 68, No. 2, 03 January 2003) of 3 February 2003.

Airlines passenger data transfer from the EU to the United States (Passenger Name Record) – frequently asked questions. Memo/03/53. Brussels, 12 March 2003.

Advanced Passenger Information – A Statement of Principles, Cairo, Egypt, ICAO, 12th Session, 22 March to 2 April 2004.

Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, Brussels, 28 November 2007.

CBP's Message Implementation Guideline for Airlines of 23 February 2009; Final Rule on Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels. DHS, CBP, 23 August 2007. 19 CFR Parts 4 and 122 [USCBP–2005–0003; CBP Dec. 07–64] RIN 1651–AA62.

Letters / Speeches

Speech/03/613 of Commissioner Frits Bolkestein addressed to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market, Strasbourg, 16 December 2003.

Letter from Commissioner Frits Bolkestein to US Secretary Tom Ridge, Department of Homeland Security, 18.12.2003.

Answer given by Mr Bolkestein on behalf of the Commission, 11 March 2004. OJ 84 E/167, 3.4.2004.

Written Testimony of Edward Hasbrouck before the LIBE Committee of the European Parliament and the Article 29 Working Party. Brussels, 26 March 2007.

Michael Chertoff, letter to Members of the European Parliament, 14 May 2007. http://useu.usmission.gov/Dossiers/Data_Privacy/May1407_Chertoff_EP_Letter.pdf.

The letter from Paul Rosenzweig, Acting Assistant Secretary for Policy at the DHS, to the EU Council Presidency, 30 July 2007. EU doc no: 12307/07.

Frattini, Franco. EU counter-terrorism strategy. European Parliament, Strasbourg, 5 September 2007.

http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/07/505.

Secondary Literature

Bignami, Francesca. *European Court of Justice Strikes EU-US Agreement on PNR Data*. 31 May 2006.
http://www.concurringopinions.com/archives/2006/05/european_court.html.

Bygrave, Lee A. *Data Protection Law: Approaching Its Rationale, Logic and Limits.* Kluwer Law International (2002).

Charlemagne. *America plays divide and rule.* Economist.com. 14 February 2008. http://www.economist.com/blogs/certainideasofeurope/2008/02/america_plays_divide_and_rule.cfm

Chertoff, Michael. *A Tool We Need to Stop the Next Airliner Plot*. Washington Post, 29.08.2006.
http://www.washingtonpost.com/wp-dyn/content/article/2006/08/28/AR2006082800849.html

Gubitz, Arnulf S. *The U.S. Aviation and Transportation Security Act of 2001 in Conflict With the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?* New England Las Review, volume 39 (2005) 446-447.

Hasbrouck, Edward. *Can you really see what records are kept about your travel?* 30.12.2008.
http://hasbrouck.org/blog/archives/001595.html.

Hasbrouck, Edward. *What's in a Passenger Name Record (PNR)?*
http://hasbrouck.org/articles/PNR.html

Ntouvas, Ioannis. *Air Passenger Data Transfer to the USA: the Decision of the ECJ and latest developments*. International Journal of Law and Information Technology, Vol. 16, Issue 1, pp. 73-95, 2008.

Peers, Steve. *The legal status of the Agreement and letters*, Statewatch, 3 July 2007.
http://www.statewatch.org/news/2007/jul/03eu-pnr.htm

Reynolds, John B. *View from Washington, European Union (EU) Privacy Directive Enters Into Force,* archived at http://www.webcitation.org/5WBIN8Xwm.

Roos, Megan. *Safe on the Ground, Exposed in the Sky: The Battle Between the United States and the European Union Over Passenger Name Information*. 14 Transnat'l L. & Contemp. Probs. 1137, 1154-55, 1161 (2005).

Waterfield, Bruno. *EU plan: The rise and rise of the securocrats*. The Daily Telegraph, 7 August 2008.
http://blogs.telegraph.co.uk/news/brunowaterfield/4841723/EU_plan_The_rise_and_rise_of_the_securocrats/

Internet Sources

Association of European Airlines
http://www.aea.be

Electronic Privacy Information Center
http://www.epic.org

EurActiv.com
http://www.euractiv.com

European Digital Rights
http://www.edri.org

Privacy International
http://www.privacyinternational.org

Statewatch
http://www.statewatch.org

Annex 1

Abbreviations:

ADIS - Arrival and Departure System
AEA - Association of European Airlines
API - Advanced Passenger Information
APIS - Advanced Passenger Information System
ATS - Automated Targeting System
BCR - Binding Corporate Rules
CAPPS - Computer Assisted Passenger Prescreening System
CBP - Customs and Border Protection, US Bureau
CoE - Council of Europe
CRS - Computerized Reservation System
DHS - Department for Homeland Security
EC - European Community
ECHR - European Convention on Human Rights
ECJ - European Court of Justice
ECTAA - European Travel Agents' and Tour Operators' Associations
EDRI - European Digital Rights Initiative
EDPS - European Data Protection Supervisor
EEA - European Economic Area
EFF - Electronic Frontier Foundation
EGF - European Gendarmerie Force
EP - European Parliament
EU - European Union
FOIA - Freedom Of Information Act
HLCG - High Level Contact Group
IATA - International Air Transportation Association
ICAO - International Civil Aviation Organization
IDP - Identity Project
INS - Immigration and Naturalization Service
MEP - Member of European Parliament
MoU - Memorandum of Understanding
PETs - Privacy-enhancing technologies
PIU - Passenger Information Units
PNR - Passenger Name Records
TSA - Transportation Security Agency
VWP - Visa Waiver Program

Annex 2

Table to the Report on 'Towards an International Infrastructure for Surveillance of Movement'

Issue	US Law Requirement	Original US Demands	EU Privacy Requirements	December 2003 Settlement
Purpose of transfer and processing?	'ensuring aviation safety and protecting national security'	'serious criminal offences'	Specific and proportionate; terrorism and serious related crime.	'Terrorism and related crimes' and to 'other serious crimes, including organized crime, of a trans-national nature'
Sharing of Data?	Beginning from the Customs Service, 'may be shared with other Federal agencies for the purpose of protecting national security'	Shared with other Federal agencies for the purpose of protecting national security, or as otherwise authorized by law.	Specific, on a case-by-case basis	Shared within the Department of Homeland Security, e.g. used in development of TSA's CAPPS system. Otherwise still very unclear, although DHS has apparently promised 'no bulk sharing with other agencies'.
How to Access Data?	'carriers shall make passenger name record information available to the Customs Service upon request.'	On-line access to Airline databases to 'pull' whatever information they wish. Includes access to non-US related travel.	Must be limited to what is strictly necessary, and limited access to sensitive information. Sharing only upon consent.	Tentative statements regarding 'push', possibly through a centralised EU institution. Possible reciprocity for the EU.
Breadth of Access to Information?	'PNR'	Broad, at the discretion of US Customs, includes non-US travel information. Estimated 50-60 fields.	Must be limited to what is strictly necessary; no access to sensitive information. Mostly information available on ticket and itinerary.	34 fields. Sensitive data to be filtered by an EU institution that will also grant access to EU member states.
Automated Processing and Profiling?	Unclear.	Data to be used within CAPPS II.	Not possible unless 'logic' of system is understood.	Leave for future agreement; even as European passenger data records are being used to develop the system.
Retention Period?	Undeclared in law.	50 years.	72-hours according to EU regulations, retained for 3 years for billing-disputes only. At most, 'a short period'; 'not more than some weeks, or even months'.	3.5 years.
Right of Redress?	none	None promised.	'Provide support and help to individual data subjects in their exercise of rights' including access to data, and Appropriate redress mechanisms for individuals'. Called for judicial or extra-judicial (independent) redress mechanisms.	CPO in DHS; possibly with EU Data Protection Authorities representing EU citizens.
Compliance Reviews?	None	None promised.	Must be ongoing verification of compliance.	Yearly with the co-operation of the EU.

Annex 3

PNR Data Elements Required by CBP from Air Carriers
(Undertakings 2004, Attachment "A"):

1. PNR record locator code
2. Date of reservation
3. Date(s) of intended travel
4. Name
5. Other names on PNR
6. Address
7. All forms of payment information
8. Billing address
9. Contact telephone numbers
10. All travel itinerary for specific PNR
11. Frequent flyer information (limited to miles flown and address(es))
12. Travel agency
13. Travel agent
14. Code share PNR information
15. Travel status of passenger
16. Split/Divided PNR information
17. Email address
18. Ticketing field information
19. General remarks
20. Ticket number
21. Seat number
22. Date of ticket issuance
23. No show history
24. Bag tag numbers
25. Go show information
26. OSI information
27. SSI/SSR information
28. Received from information
29. All historical changes to the PNR
30. Number of travelers on PNR
31. Seat information
32. One-way tickets
33. Any collected APIS information
34. ATFQ fields

Types of EU PNR Collected
(PNR Agreement 2007):

1. PNR record locator code
2. Date of reservation/ issue of ticket
3. Date(s) of intended travel
4. Name(s)
5 Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.)
6. Other names on PNR, including number of travelers on PNR
7. All available contact information (including originator information)
8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)
9. Travel itinerary for specific PNR
10. Travel agency/travel agent
11. Code share information
12. Split/divided information
13. Travel status of passenger (including confirmations and check-in status)
14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote
15. All Baggage information
16. Seat information, including seat number
17. General remarks including OSI, SSI and SSR information
18. Any collected APIS information
19. All historical changes to the PNR listed in numbers 1 to 18